Caveats in Cisco IOS XE 3.1S Releases

This chapter provides information about caveats in Cisco IOS XE 3.1S 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 section:

Caveats in Cisco IOS XE 3.1S 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 3.1S 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.)

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 consists of the following subsections:

Resolved Caveats—Cisco IOS XE Release 3.1.4aS

The following are the resolved caveats in Cisco IOS XE Release 3.1.4S:

- 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.

- CSCtr22007

  Symptoms: A Cisco 7600 router that is configured with RSVP crashes.

  Conditions: MPLS-TE Tunnel Flap.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.1.4S

The following are the open caveats in Cisco IOS XE Release 3.1.4S:

- CSCtg59243

  Symptom: The Hot ICE Before After feature stops working when you run the **mpls static binding ipv4** LDP command.

  Conditions: This issue is observed when you run the **mpls static binding ipv4** command.

  Workaround: There is no workaround.

- CSCto49680

  Symptom: On a traffic class that is fitted with a time-range access list, the traffic keeps meeting the matching criteria even when the access list is inactive.

  Conditions: This issue is observed a few days after a traffic class is fitted with a time-range access list.

  Workaround: There is no workaround.

- CSCtq56709

  Symptom: The Cisco ASR 1000 ESP reloads automatically.

  Conditions: This issue is observed on an ISG under high-load conditions.

  Workaround: There is no workaround.

- CSCto77352

  Symptom: The standby RP cannot reach the hot synchronization state with the active RP. The standby RP continues to reload automatically, and the following message is displayed:

  ```
  *Apr 18 15:38:47.704: %SYS-3-CPUHOG: Task is running for (3305)msecs, more than
  (2000)msecs (1/1),process = IPC Dynamic Cache.
  ```

  Conditions: This issue is observed in the stateful switchover (SSO) mode, when the ISG is configured as the DHCP server, and the DHCP lease time is set to a low value.

  Workaround: There is no workaround.

- CSCtn62287

  Symptom: The standby router may crash when an interface flaps or while performing a soft OIR of the SPA.

  Conditions: This issue is observed when interfaces are bundled as a multlink and traffic is flowing across the multilink.

  Workaround: There is no workaround.

- CSCtq86244

  Symptom: After an SSO, ISIS does not send its topology database to the TE. Therefore, the TE cannot determine the path to the destination of the tunnels and the tunnel stays down.

  Conditions: This issue is observed when the ISIS is configured with the **nsf cisco** command and the TE is not configured for high availability.

  Workaround: Run the **nsf ietf** command on the ISIS.

- 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.

- CSCtr26226

  Symptoms: The RP and SIP crash.

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

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.1.4S

The following are the resolved caveats in Cisco IOS XE Release 3.1.4S:

- CSCtb24959

  Symptom: The router may crash while a large number of RP mappings are being cleared.

  Conditions: This issue is observed when you configure the router as an RP agent and candidate RP for a large number of RPs. The router may crash when you run the **clear ip pim rp-map** command multiples times.

  Workaround: Do not run the **clear ip pim rp-map** command multiples times.

- CSCth90147

  Symptom: The router responds to a router solicitation message with a router advertisement message.

  Conditions: This issue is observed when you run the **ipv6 nd ra suppress** command. This command is only intended to suppress periodic multicast router advertisement messages. The router continues to respond to unicast router solicitation messages, which is the intended behavior.

  Workaround: Use an ACL to block the reception of router solicitation packets.

- CSCti87194

  Symptom: When a long IPC message is fragmented, the last fragment causes a crash because of an invalid zone value.

  Conditions: This issue is observed when a long IPC message is fragmented.

Workaround: There is no workaround.

- CSCti91029

  Symptom: A traceback occurs, and the following message is displayed:

  ```
  %INFRA-3-INVALID_GPM_ACCESS: Invalid GPM ...
  ```

  Conditions: This issue is observed when NAT configuration commands or NAT EXEC commands are run after the **debug ip nat** *aclnum* command is run.

  Workaround: There is no workaround.

- CSCtj20776

  Symptom: When a RADIUS proxy session is reauthenticated, the Accounting Stop record is sent for the session.

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

  - The authentication request comes from the AP.
  - The accounting request comes from the AZR, and the session on the ISG is associated with the AZR.
  - The ISG receives a reauthentication request from the AP.
  - The acct-terminate-cause field in the Stop record is set to none.

  The Accounting Stop record is sent for the RADIUS proxy session and the services under the session. However, note that the RADIUS proxy session is still active and a Stop record is not sent for the session when the session is cleared.

  Workaround: There is no workaround.

- CSCtj30155

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

  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

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

- CSCtj44374 and CSCti70931

  Symptom: When you try to configure the router through Telnet access (vty), the router stops responding. The console is active, but not responsive. When the **show processes cpu** command is run, the output shows high CPU utilization.

  Conditions: This issue is observed when you configure 200 or more call policy sets, with each policy set containing a large number of entries.

  Workaround: Do not create more than 100 entries in each call policy set.

- CSCtj58672

  Symptom: The MallocLite memory leak occurs when the vlan_bl_util_process_bitlist function is called.

Conditions: This issue is observed when the L3VPN and BFD profile configuration is set on the router.

Workaround: There is no workaround.

- CSCtj87846

  Symptom: A subinterface that is in the Up state is considered to be in the Down state by the PfR master controller.

  Conditions: This issue is observed under either of the following conditions:

  - A subinterface is used as an external interface and the corresponding physical interface goes down and then comes up.
  - The router is reloaded.

  Under either condition, the PfR master controller is not notified that the subinterface has returned to the Up state.

  Workaround: Run the **clear pfr master *** command on the PfR master controller.

- CSCtj92247

  Symptom: The standby RP reloads automatically because the configuration is not in synchronization with the primary RP.

  Conditions: This issue is observed when you modify the parameters, for example, the peak value, of a VP.

  Workaround: There is no workaround.

- CSCtk76697

  Symptom: After a test crash on a line card, the first 100-odd service instances out of 4000 service instances on the line card change to the Down state. This results in a complete traffic drop on these service instances.

  Conditions: This issue is observed only during the first test crash on the LC after the router is booted.

  Workaround: Run the **shut** and **no shut** commands on the service instance or the interface.

- CSCtl67150

  Symptom: PPP multilink interfaces do not come up on the serial interface.

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

  - T1 channel groups are created in a CT3 interface.
  - A multilink interface is created.
  - One link is created per channel group.
  - CHAP authentication is applied when PPP encapsulation is used for each link.

  Workaround: There is no workaround.

- CSCtl84797

  Symptom: SBC traceback occurs.

  Conditions: This issue is observed when Lawful Intercept (LI) is enabled and there are multiple media sessions in a single call, that is, SDP contains information about multiple media sessions.

  Workaround: There is no workaround.

- CSCtn15317

Symptom: Traffic on the MPLS VPN is dropped. The LFIB entry on the P router contains an instruction to TAG all the packets that are destined for the PE router instead of the POP instruction that is expected on a directly connected P router.

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

- The ISIS protocol is running as IGP on MPLS infrastructure.
- ISIS on the PE router is a summarizing network that includes the BGP VPNv4 Update Source configuration.
- The P router is running an MFI-based image.

Workaround: Remove the **summary-address** configuration from ISIS on the PE router, and change the BGP update source.

- CSCtn19178

  Symptom: If you are running an Inter-AS MPLS design across two autonomous systems, the router may clear the local label for a working VRF and a new local label is not reassigned.

  Conditions: This issue is observed on the MPLS Edge LSR when you remove the configuration of an unused VRF, including either of the following:

  - The VRF interface, for example, by running the **no interface Gi1/0/1.430** command.
  - The same VRF process, for example, by running the **no router ospf** *process-id* **vrf** *vrf-name* command.

  Run the **show ip bgp vpnv4 vrf A subnet** command on the working VRF to verify whether you are facing this issue.

  Workaround: To reprogram a new local label on the PE router, clear the MP-BGP session by using one of the following commands:

  - **clear ip bgp mp-bgp neighbor soft in clear**
  - **ip bgp mp-bgp neighbor soft out**

- CSCtn22728

  Symptom: When the **exit** command is run in the EVC mode, the standby RP may reload automatically due to configuration synchronization and the following error message may be displayed:

  ```
  %PFREDUN-SP-STDBY-6-STANDBY: Ready for SSO mode    Config Sync: Line-by-Line sync
  verifying  failure on command: exi exi due to parser return error rf_reload_peer_stub:
  RP sending reload request to Standby. User: Config-Sync, Reason: Configuration
  mismatch
  ```

  Conditions: This issue is observed when an unsupported interface CLI option is used with the **destination** keyword in the ERSPAN source session configuration.

  Workaround: There is no workaround. Do not run commands such as the **exit** command that are not applicable to the EVC mode.

- CSCtn38996

  Symptom: MVPN traffic is lost when a peer is reachable using a TE tunnel and an interface flap is performed to enable the selection of the secondary path. The multicast route does not contain a native path that uses the physical interface.

  Conditions: This issue is observed when the **mpls traffic-eng multicast-intact** command is configured under OSPF.

  Workaround: Run the **clear ip ospf process** command on the core router.

- CSCtn48009

  Symptom: A Cisco ASR 1000 series router may experience unexpected periodic ESP reloads at regular intervals (that is, every X hours and Y minutes). The issue is specific to an ESP such that the problem will follow that ESP if moved to a different slot and/or chassis. Note that Cisco IOS images with this change will still experience periodic reloads although the reporting will more clearly indicate the cause.

  Conditions: This symptom is observed with any Cisco ASR 1000 series router with a persistent error in the QFP memory.

  Workaround: There is no workaround. The affected ESP board or the Cisco ASR 1001 router must be replaced.

- CSCtn53222

  Symptom: Real servers, such as ASNGW, GGSN, and RADIUS, are stuck in the READY_TO_TEST state and do not switch to the OPERATIONAL state.

  Conditions: This issue is observed when a real server moves to the FAILED state because of real server failure that is detected by the inband failure mechanism. After the retry timeout interval, the real server is moved to the READY_TO_TEST state.

  Workaround: Change the state of the real server to OUTOFSERVICE and then to INSERVICE.

- CSCtn56526

  Symptom: The MBS is always calculated on the basis of the MTU value. The user-defined MBS value is not included in the output of the **show atm pvc** command.

  Conditions: This issue is observed when the MBS is configured using the CLI and the **show atm pvc** command is run.

  Workaround: There is no workaround.

- CSCtn64500

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

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

  Workaround: Run the **clear adjacency** command to force-repopulate the incomplete adjacency.

Note Note that the **clear adjacency** command has a system-wide impact. As an alternative, you can use unicast commutation.

- CSCtn65599

  Symptom: Some multicast streams from the CE router are not forwarded to the Data MDT by the PE router.

  Conditions: This issue is observed after an SSO or a PRE crash.

  Workaround: There is no workaround.

- CSCtn73941

  Symptom: After performing an OIR for an ES card having EVC configuration with the **module clear-config** command enabled, restoring the old configuration does not work. This indicates that traffic will not be forwarded over those service instances. In addition, VLANs used in the previous configuration cannot be effectively used on those ports.

Conditions: This issue is observed when you run the **module clear-config** command.

Workaround: There is no workaround.

- CSCtn74673

  Symptom: After a reload, incoming multicast traffic is punted into the CPU before MFIB is downloaded to the line cards. Because of the high CPU rate, the line cards are stuck in a continual loop of failing to complete the MFIB download.

  Conditions: This issue is observed when high CPU utilization is caused by the multicast traffic. The **show mfib linecard** command does not show the line cards in synchronization with each other and the tables are in the connecting state.

  Workaround: Reload the line cards.

- CSCtn95344

  Symptom: The standby RSP gets stuck in RF progression at cold bulk while booting.

  Conditions: This issue is observed after the RPR is downgraded from Release 12.2(33)SRE2 to Release 12.2(33)SRE1.

  Workaround: Reload the router.

- CSCtn96521

  Symptom: When the spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors are not able to establish an adjacency.

  Conditions: This issue is observed when the spoke peer group is configured before the iBGP peer group.

  Workaround: Configure the iBGP peer group before the spoke peer group.

- CSCtn97451

  Symptom: The BGP peer router crashes when the **clear bgp ipv4 unicast peer** command is run.

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

  – Internal BGP is running between Router 1 and Router 2.
  – External BGP is running between Router 1 and Router 3.
  – Traffic is travelling from Router 3 to Router 2.
  – The **clear bgp ipv4 unicast peer** command is run on Router 2.

  Workaround: There is no workaround.

- CSCtn98642

  Symptom: The RP crashes, and the following error message is displayed:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Ether-SPA background
  process
  ```

  Conditions: This issue is observed when QinQ (min 50) and QinQ-Any with the same outer VLAN is present and both the following conditions are met:

  – A large-scale configuration has QinQ and QinQ-Any with the same outer VLAN on SPA.
  – The router is reloaded.

  Workaround: There is no workaround.

- CSCto02448

  Symptom: The AS-PATH attribute is lost after an inbound route refresh is performed.

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

- The neighbor is configured with soft-reconfiguration inbound.
- The inbound routemap is not configured for the neighbor.
- The nonroutemap inbound policy (filter list) allows the path.

Workaround: Use the routemap inbound policy to filter the prefixes.

- 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

- CSCto07586

  Symptom: An IPv4 static BFD session does not get established on a system that does not have IPv6 enabled.

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

  - The router does not have IPv6 enabled.
  - BFD is enabled on an interface.
  - An IPv4 static route is configured with BFD routing through the interface.

  The IPV4 BFD session does not get established, and as a result, the static route does not get installed.

  Workaround: Unconfigure and then reconfigure BFD on the interface.

- CSCto07919

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

  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

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

- CSCto10336

  Symptom: The LNS router stops responding at the interrupt level.

  Conditions: This issue is observed during control channel cleanup.

  Workaround: There is no workaround.

- CSCto15361

  Symptom: The Active Supervisor crashes when the **router eigrp** configuration is removed.

  Conditions: This issue is observed because the EIGRP Hello process is stopped while disabling the IPv6 router EIGRP.

  Workaround: Modify the igrp2_procinfo_free function to stop the EIGRP Hello process before cleaning up the peer list.

- CSCto16106

  Symptom: An address is not assigned when the **ip dhcp use class aaa** command is run.

  Conditions: This issue is observed when the DHCP server is configured to download a class name from the RADIUS server by using the **ip dhcp use class aaa** command and to lease an IP address from that class. The IP address is not assigned to the client.

  Workaround: There is no workaround.

- CSCto31265

  Symptom: The Area Border Router (ABR) does not translate Type 7 LSA when the primary Type 7 LSA is deleted, even if another Type 7 LSA is available.

  Conditions: This issue is observed when you are using OSPFv3 and the ABR receives multiple Type 7 LSAs for the same prefix from multiple ASBRs.

  Workaround: Perform one of the following steps:

  - Delete and then add the static route that generates Type 7.
  - Run the **clear ipv6 ospf force-spf** command on the ABR.
  - Run the **clear ipv6 ospf redistribution** command on the ASBR.

- CSCto41165

  Symptom: The standby router reloads automatically when you use the **ip extcommunity-list 55 permit | deny** command and then run the **no ip extcommunity-list 55 permit|deny** command.

  Conditions: This issue is observed when the standby router is configured.

  Workaround: There is no workaround.

- CSCto44585

  Symptom: Packets with the DF bit set across the L2TPv3 tunnel are punted or dropped on the CPU.

  Conditions: This issue is observed when the PMTU in the pseudowire class configuration is enabled.

  Workaround: Reduce MTU on the client side.

- CSCto46716

  Symptom: Routes over the MPLS TE tunnel are not present in the routing table.

  Conditions: This issue is observed when the MPLS TE tunnel is configured with forwarding adjacency. If you run the **debug ip ospf spf** command while the SPF process link for the TE tunnel is in its own RTR LSA, the `Add path fails: no output interface` message is displayed.

Note Some tunnels are not affected when the MPLS TE tunnel is configured with the forwarding adjacency. However, it is not always possible to identify the tunnel that is affected. The number of affected tunnels increases with the number of configured tunnels.

Workaround: Use the **autoroute announce** command instead of the **forwarding-adjacency** command.

- CSCto52235

  Symptom: The MAC address accounting commands cannot be used.

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

  Workaround: There is no workaround.

- CSCto55643

  Symptom: High CPU loading conditions can result in delayed download of multicast routes to the line cards, resulting in the MFIB state on the line cards that are not in synchronization with the RP. The **show mfib linecard** command shows line cards in the Sync Fail state and the LOADED state.

  Conditions: This issue is observed when there is high CPU load due to router reload or line card OIR events in a highly scaled multicast environment with high line rates of multicast traffic and unrestricted process-switched packets.

  Workaround: There is no workaround.

- CSCto55983

  Symptom: After a reload, incoming multicast traffic is punted into the CPU before MFIB is downloaded into the line cards. Because of the high CPU rate, line cards are stuck in a continual loop of failing to complete MFIB download and retrying.

  Conditions: This issue is observed during high CPU utilization caused by multicast traffic. The **show mfib line summary** command does not show cards in synchronization.

  Workaround: There is no workaround.

- CSCto72480

  Symptom: The output of the **show mfib linecard** command shows that line cards are in the Sync Fail state.

  Conditions: This issue is observed when the last reload context displayed in the output of the **show mfib linecard internal** command is epoch change. This indicates that an IPC timeout error has occurred in the communications channel (MRIB), which downloads multicast routing entries to the MFIB. In this scenario, multicast routing changes are not communicated to the failed line cards and are not synchronized with the RP.

  Workaround: Run the **clear mfib linecard** command.

Note The workaround may not work if high CPU utilization continues to be present and IPC errors are reported.

- CSCto74038

  Symptom: After an upgrade, the CESoPSN (clock) pseudowire stays in the Down state due to payload size value mismatch.

Conditions: Before upgrading, the payload size is configured to 80 and the dejitter value is the default (5). This issue is observed if you configure the payload size or dijitter value to a value other than the default and upgrade the system.

Workaround: Set the payload size and dejitter value to their defaults.

- CSCtq09088

  Symptom: The router crashes while trying to run the **ip rsvp sender-host** command. For example:

  ip rsvp sender-host 203.0.113.26 203.0.113.65 UDP 11 11 10 10 identity bogusID

  Conditions: This issue is observed when the **ip rsvp sender-host** command is run.

  Workaround: There is no workaround.

- CSCtf81249

  Symptom: Memory leaks are observed while running configuration commands.

  Conditions: This issue is observed only when the Tcl shell is used.

  Workaround: Run the **end** command.

- CSCtl90292

  Symptom: The following error messages are displayed:

  ```
  an 18 08:00:16.577 MET: %SYS-2-MALLOCFAIL: Memory allocation of 9420 bytes failed from
  0x42446470, alignment 32  Pool: I/O Free: 11331600  Cause: Memory fragmentation
  Alternate Pool: None  Free: 0  Cause: No Alternate pool  -Process= "BGP I/O", ipl= 0,
  pid= 564   -Traceback= 417E8BEC 4180FA6C 42446478 42446B64 42443984 40FC18C8 40FCCB4C
  40FD1964 403BDBFC 403BCC34 40344508 403668AC
  ```

  Conditions: This issue is observed when a large number of hits and failures are observed in the medium buffers and all are of link-type IPC. For example:

  ```
  buffer information for Medium buffer at 0x4660E964  ...    linktype 69 (IPC), enctype
  1 (ARPA), encsize 14, rxtype 0 if_input 0x481DEA50 (EOBC0/0), if_output 0x0 (None)
  ```

  Workaround: There is no workaround.

- CSCtq36726

  Symptom: Configuring the **ip nat inside** command on the IPSec dVTI VTEMP interface does not have any effect on the cloned virtual access interface. The NAT feature does not work because the virtual access interface does not get this command cloned from its corresponding VTEMP.

  Conditions: This issue is observed on a router with dVTI-based IKEv2 configured.

  Workaround: Reconfigure the virtual template interface so that the **ip nat inside** command is applied first.

- CSCtq83629

  Symptom: When an IPC error occurs, another error associated with a loss in the multicast forwarding state on line cards under scaled conditions occurs.

  Conditions: This issue is observed when either of the following conditions is met:

  - The router is booted.
  - A high CPU load causes IPC timeout errors. The issue occurs on line cards during recovery from an IPC error in the MRIB channel.

  Workaround: There is no workaround. A line card reload might resolve the issue.

Open Caveats—Cisco IOS XE Release 3.1.3S

The following are the open caveats in Cisco IOS XE Release 3.1.3S:

- CSCsk80075

  Symptom: On a router with the SSO High Availability mode enabled, when the **no interface multilink** command is used to remove a multilink interface from the configuration, the standby RP may automatically reload.

  Conditions: This issue is observed when the multilink interface is active and the **shutdown** and **no interface multilink** commands are run in quick succession on the multilink interface.

  Workaround: After running the **shutdown** command, wait for a few seconds before running the **no interface multilink** command.

- CSCtd08709

  Symptom: When an LTS is restricted, CAC calls are not terminated through another LTS.

  Conditions: This issue is observed when an LTS is restricted.

  Workaround: Do not restrict CAC on the LTS.

- CSCtd87072

  Symptom: The router reboots when the tunnel mode is changed in scaled IPSec sessions.

  Conditions: This issue is observed when the tunnel mode is changed in scaled IPSec sessions.

  Workaround: There is no workaround.

- CSCtf39056

  Symptom: On a router running Cisco IOS 12.2(33)XND, RRI routes are not deleted automatically after the SA is cleared.

  Conditions: This issue is observed on a router running Cisco IOS 12.2(33)XND.

  Workaround: There is no workaround.

- CSCtf54919

  Symptom: The router crashes and CPU hog messages are displayed.

  Conditions: This issue is observed when the virtual access interface is shut down.

  Workaround: Apply one of the following workarounds:

  - When you remove an access list, remove the corresponding distribute list configuration.
  - Do not use the same access list name for both IPv4 and IPv6.

- CSCtf71673

  Symptom: A PRE crash occurs due to memory corruption with block overrun.

  Conditions: This issue is observed during PTA and L2TP access.

  Workaround: There is no workaround.

- CSCtj46496

  Symptom: When multiple physical OIR of the RP and ESP are performed at the same time, the RP might experience keepalive packet loss and then crash. Traffic issues might also be observed before the RP crashes.

  Conditions: This issue is observed when multiple physical OIR of the RP and ESP are performed at the same time. Note that this issue does not occur when a soft OIR is performed.

Workaround: There is no workaround.

- CSCtj94121

  Symptom: The RADIUS extended process leaks memory.

  Conditions: This issue is observed if the LNS is configured and the RADIUS extended process is in use.

  Workaround: There is no workaround.

- CSCtj96760

  Symptom: Unable to ping all bundles with **dlfi over atm in scaled configs in cwpa2.**

  Conditions: This issue is observed when more than 250 VT are created.

  Workaround: There is no workaround.

- CSCtk05142

  Symptom: Slow speed and increased latency is observed on the data path.

  Conditions: This issue is observed when a zone-based firewall is configured and a single high-volume flow is directed at the router when the firewall is enabled.

  Workaround: There is no workaround.

- CSCtk76228

  Symptom: When the **hw-module slot f0 reload** command is used during an FP switchover, the following error message is displayed:

  ```
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp:  cpp_cp encountered an error
  ```

  Conditions: This issue is observed with the scaling configuration when there are a large number (for example, 8000 or more) of virtual circuits.

  Workaround: There is no workaround.

- CSCtl09030

  Symptom: The router crashes during the ARP input process.

  Conditions: This issue is observed when all of the following conditions exist at the same time:

  - The router is configured with the DHCP pool to function as the server for some clients and as the relay for other clients.
  - The DHCP database agent is enabled.
  - The ISG in-band IP session initiator is configured.
  - An ARP request is received from a client whose lease has expired.

  Workaround: There is no workaround.

- CSCtl70143

  Symptom: At times, the LAC does not forward the `PPP CHAP-SUCCESS` message from the LNS to the client.

  Conditions: This issue is observed when T1(PRI) is used between the LAC and the client.

  Workaround: There is no workaround.

- CSCtl70677

  Symptom: The FMAP FP crashes when the following command is run:

show platform hardware qfp active infrastructure shared-memory process forwarding-manager

Conditions: This issue is observed when the command mentioned in the Symptom description is run.

Workaround: There is no workaround.

- CSCtn11144

  Symptom: A QFP crash occurs.

  Conditions: This issue is observed when features such as MLP, VFR, and fragmentation and reassembly are used.

  Workaround: There is no workaround.

- CSCtn15317

  Symptom: Traffic on the MPLS VPN is dropped. In the LFIB entry on a P router, there is an instruction to tag all packets that are destined for the PE router instead of a POP instruction that is expected on a directly connected P router.

  Conditions: This issue is observed when all the following conditions exist at the same time:

  – The IS-IS protocol is running as IGP on MPLS infrastructure.
  – The IS-IS protocol on the PE router is summarizing the network that includes the BGP VPNv4 update source.
  – The P router is running an MFI-based image.

  Workaround: Apply one of the following workarounds:

  – Remove the summary address command in IS-IS on the PE.
  – Change the BGP update source.

- CSCtn19444

  Symptom: mLACP member links may be bundled on an isolated PoA with a core failure. This results in both PoAs becoming active.

  Conditions: This issue is observed while running mLACP and the ICRM connection between the PoAs is lost.

  Workaround: Set up shared control by configuring **lacp max-bundle** on the dual-homed device (DHD) if the device supports it. This prevents the DHD from bundling the member links to both PoAs at the same time.

- CSCtn25290

  Symptom: If the router is configured as a 6rd CE with **tunnel 6rd br** set, it cannot communicate with other CEs.

  Conditions: This issue is observed when the router is configured as a 6rd CE with **tunnel 6rd br** set.

  Workaround: There is no workaround.

- CSCtn38996

  Symptom: MVPN traffic is lost even when the peer is reachable using a TE Tunnel and an interface flap is performed so that the secondary path can be selected but the multicast route does not contain a native path using the physical interface.

  Conditions: This issue is observed when **mpls traffic-eng multicast-intact** is configured under OSPF.

  Workaround: Run the **clear ip ospf process** command on the core router.

- CSCtn43795

  Symptom: A coredump may occur in the CPP client.

  Conditions: This issue is observed when a CEF object is reparented and the previous parent is requested to delete itself. The delete operation of the parent might be carried out before the modify operation of the child is completed.

  Workaround: To avoid the reparenting operation, do not use the **copy config** command.

- CSCtn44347

  Symptom: The FP40 crashes.

  Conditions: This issue is observed while configuring the route map on the router.

  Workaround: There is no workaround.

- CSCtn48009

  Symptom: The ESP crashes periodically, and the **%CPPOSLIB-3-ERROR_NOTIFY: F0** error message is displayed.

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

  Workaround: There is no workaround.

- CSCtn52207

  Symptom: After an SSO, the MIB reports some extra instances. No messages are displayed on the console for these extra instances.

  Conditions: This issue is observed after an SSO is performed.

  Workaround: There is no workaround.

- CSCtn54703

  Symptom: The shape rate limit is exceeded for priority traffic.

  Conditions: This issue is observed when the same three-level service policy is configured on both a 10-Gigabit Ethernet and a 1-Gigabit Ethernet interface. When this happens, at times, the parent shape rate is not applied while sending priority traffic.

  Workaround: Use a different service policy on each interface. In addition, ensure that the parent shape rate set for the two interfaces is not the same.

- CSCtn57731

  Symptom: The ESP is automatically reloaded while removing the tunnel interface configuration.

  Conditions: This issue is observed when the router functions as an IPSec termination and aggregation router for DMVPN hub deployment and when IVRF is not equal to FVRF.

  Workaround: There is no workaround.

- 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

- CSCto21732

  Symptom: When the Cisco ASR 1006 Router or Cisco ASR 1013 Router is started, the standby console does not show the `stby` extension in the host name.

  Conditions: This issue is observed when the Cisco ASR 1006 Router or Cisco ASR 1013 Router is booted with hardware redundancy with an RP2 adventerprise image (for example, asr1000rp2-adventerprise.03.01.03.S.150-1.S3.bin).

  Workaround: Use the **hostname** command to change the host name.

Resolved Caveats—Cisco IOS XE Release 3.1.3S

The following are the resolved caveats in Cisco IOS XE Release 3.1.3S:

- CSCsl18054

  Symptom: A local user created with a one-time keyword is automatically removed after failed login attempts. The expected behavior is that the one-time user should be removed after the first successful login, not after failed login attempts.

  Conditions: This issue is observed on a router running Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCsy61302

  Symptom: Chunk header corruption occurs, and the router crashes. The `BADMAGIC` error message is displayed for a chunk that is either free or in use.

  Conditions: This issue is observed when the following SNMP commands are configured:

  snmp-server community public ro

  snmp-server packetsize 17940

  Workaround: Do not set the packet size to a value greater than 2048.

- CSCtd59027

  Symptom: The router crashes due to a bus error.

  Conditions: This issue is observed when crypto is configured and running on the router. The issue may be linked to EzVPN.

  Workaround: There is no workaround.

- CSCtd72318

  Symptom: The Cisco ASR 1004 Router crashes at __be_dhcpc_for_us.

  Conditions: This issue is observed on a router running Cisco IOS Release 12.2(33)XNC2. The issue may be associated with DHCP configuration.

  Workaround: There is no workaround.

- CSCte36327

  Symptom: On the Cisco ASR 1002 Router, the standby RP is automatically rebooted at startup.

  Conditions: This issue is observed on the Cisco ASR 1002 Router.

  Workaround: There is no workaround.

- CSCtf11309

  Symptom: If the MFR interface has a policy map attached to it, the interface flaps when it is shut down and restarted.

  Conditions: This issue is observed when the MFR interface has a policy map attached to it.

  Workaround: There is no workaround.

- CSCtf23298

  Symptom: CPU usage is high when a TACACS server is configured with a single connection.

  Conditions: This issue is observed when the TACACS server is configured with a single connection.

  Workaround: Remove the single connection option.

- CSCtf72328

  Symptom: BFD IPv4 Static does not fully support the Admin Down state.

  Conditions: This issue is observed when the static route is deleted from the BFD neighbor.

  Workaround: Shut down and then restart the interface on which the BFD session is configured.

- CSCtf83711

  Symptom: A memory leak occurs after PPPoE sessions are tested.

  Conditions: This issue is observed after PPPoE sessions are tested.

  Workaround: There is no workaround.

- CSCtf90182

  Symptom: When a subinterface based PW (EoMPLS) is configured on SIP400, an SSO causes a traffic drop of 80 seconds. The VC on the peer router does not come up quickly. It goes to the Down state and then comes back up after 80 seconds.

  Conditions: This issue is observed during an SSO, when both LDP GR and OSPF NSF AWARE are configured.

  Workaround: Configure a longer hello holdtime when you run the following command:

  mpls ldp discovery hello holdtime *holdtime_value*

- CSCtg59328

  Symptom: When IPCP renegotiates for an existing PPPoE session, the new IPv4 address is not synchronized with the standby RP.

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

  1. Open a PPPoE session, and ensure that it is synchronized with the standby RP.
  2. From the PPPoE client, run the **no ip address** command followed by the **ip address negotiated** command under the virtual template interface.

  When the **no ip address** command is run, the session first switches to the Down state on both the active and standby RPs. The **ip address negotiated** command then triggers IPCP renegotiation, and the session switches to the Active state. However, on the standby RP, the session remains in the Down state and the new IP address is not synchronized.

Workaround: There is no workaround.

- CSCtg78106

  Symptom: Even when SNMP is not configured on the router, the router shows SNMP ports as open or there are responses to SNMP requests.

  Conditions: This issue is observed when a specific set of configuration events are performed. To check whether the router is affected by this issue, run the **show ip sockets** or **show control-plane host open-ports** command. If the output of the command shows that the UDP 161 and UDP 162 SNMP ports are open and listening, run the **show running-config | include snmp** command. If this command does not return any output, it is confirmed that the router is affected by this issue.

  Workaround: Close the ports by performing the following steps:

  1. Configure an SNMP community. For example:

     snmp-server community workaround

  2. Use the **show snmp community** command to display the names of existing SNMP communities.
  3. Remove each SNMP community name by running the following command:

     no snmp-server community "*community_name***"**

  4. Shut down the SNMP agent by running the following command:

     no snmp-server

- CSCth03022

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

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

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

- CSCth14305

  Symptom: If a bandwidth statement is configured on a multilink bundle interface and if the link members flap, changes in bandwidth are not handled correctly. This causes issues in QoS and BQS.

  Conditions: This issue is observed when a bandwidth statement is configured on a multilink bundle interface.

  Workaround: There is no workaround.

- CSCth25634

  Symptom: When logging in, a user is prompted for a password two times.

  Conditions: This issue is observed when login authentication has the line password configured as the fallback and the RADIUS password as the primary.

  Workaround: To change the login authentication to fall back to the enable password that is configured on the UUT, use a command similar to the following command:

  enable password *keyword* **aaa authentication login default group radius enable**

- CSCth37580

Symptom: A dampening route is present even after the BGP dampening configuration is removed.

Conditions: This issue is observed when the following sequence of events takes place:

1. DUT connects to RTRA with eBGP VPNv4.
2. An eBGP VPNv4 peer session is established and DUT.
3. DUT has the VRF (that is, the same RD) as the route advertised by RTRA.

In this scenario, when DUT learns the route, it imports the same RD and the topology of the network is changed from VPNv4 to VRF.

Workaround: There is no workaround.

- CSCth45731

  Symptom: PPPoE sessions are partially synchronized with the standby RP. Later, these sessions are not cleaned up.

  Conditions: This issue is observed when IPCP is renegotiated and then terminated before full session synchronization is performed for the PPPoE session that is starting.

  Workaround: There is no workaround.

- CSCth45774

  Symptom: The router crashes when the **no ip policy routemap** command is run on multiple interfaces.

  Conditions: This issue is observed when the route map does not exist.

  Workaround: Remove the policy configuration before removing the route map.

- CSCth66177

  Symptom: If the standby PRE crashes, the active PRE also crashes.

  Conditions: This issue is observed when the standby PRE crashes due to memory parity error. The standby PRE crash triggers an active PRE crash due to bus error.

  Workaround: There is no workaround.

- CSCth69364

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCti48504

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

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

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

- CSCti18615

Symptom: Reloading a router with multicast forwarding configured may result in the standby RP getting out of synchronization with the active RP. When this happens, the A and F flags are not included in the multicast forwarding base entries.

Conditions: This issue is observed when multicast forwarding is operational and configured in the startup-config file, the router is in High-Availability-mode SSO, and the router is reloaded from the RP.

Workaround: Shutting down and restarting the affected interfaces may fix the issue.

- CSCti34396

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

  Conditions: This issue is observed when **next-hop-unchanged allpaths** is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is unreachable.

  Workaround: Configure a route map to rewrite routes so that the tunnel endpoint is an address that is reachable from both inside and outside the VRF.

- CSCti61949

  Symptom: The router is automatically reloaded, and the following error messages are displayed:

  ```
  SYS-2-CHUNKBADMAGIC: Bad magic number in  chunk header
  chunk name is BGP (3) update
  ```

  Conditions: This issue is observed while receiving BGP updates from a speaker for a multicast-enabled VRF.

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

- CSCti85446

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

  Conditions: This issue is observed when the nexthop static route is configured with a permanent keyword.

  Workaround: Delete all static routes that pass through the affected nexthop, and then add them again.

- CSCti98931

  Symptom: Some sessions may be lost after an L2TP switchover.

  Conditions: This issue is observed after an L2TP switchover.

  Workaround: There is no workaround.

- CSCtj08533

  Symptom: QoS classification fails on egress PE if the route is learned through BGP.

  Conditions: This issue is observed when there are redundant paths to the CPE.

  Workaround: Use only one path between PE and CPE.

- CSCtj17545

  Symptom: After a switchover, the restarting speaker sends TCP-FIN to the receiving speaker, when receiving speaker tries to establish (Active open). This may cause packets to be dropped.

  Conditions: This issue is observed when a large number of BGP peers are set up on different interfaces.

  Workaround: Configure the receiving speaker to accept passive connections.

- CSCtj24453

  Symptom: A traceback message is displayed when the **clear ip bgp *** command is run.

  Conditions: This issue is observed when there are a large number of routes and route map cache entries.

  Workaround: Run the **no bgp route-map-cache** command to ensure that route map results are not cached.

- CSCtj30462

  Symptom: Details of subscribers are not correct.

  Conditions: This issue is observed under any one of the following conditions:

  - High system usage.
  - Incorrect download of a previous service.
  - The same subscriber is present in two different PPPoE sessions.

  Workaround: There is no workaround.

- CSCtj48629

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

  Conditions: This issue is observed on a router running Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCtj58943

  Symptom: When the **encapsulation dot1q 1381** command is used, the standby RP reloads due to line-by-line synchronization failure.

  Conditions: This issue is observed when a configuration command is run under a subinterface mode.

  Workaround: There is no workaround.

- CSCtj61748

  Symptom: Service activation may fail.

  Conditions: This issue is observed when there are multiple services in the session authentication and authorization response.

  Workaround: Remove the Service Group and Service Type fields from the service definitions.

- CSCtj65553

  Symptom: A static route that is installed in the default table is automatically removed.

  Conditions: This issue is observed after a RP to line card to RP transition.

  Workaround: Add the missing static route.

- CSCtj77004

  Symptom: While PPPoE sessions are getting established, the archive log configuration size impacts CPU utilization. In addition, only some configuration lines from the virtual template are copied to the archive. The remaining configuration files are not copied.

  Conditions: This issue is observed when **archive log config** is configured.

  Workaround: There is no workaround.

- CSCtj82292

  Symptom: The EIGRP summary address with AD 255 is sent to a peer.

Conditions: This issue is observed when the summary address is advertised as follows:

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

Workaround: There is no workaround.

- CSCtj87180

  Symptom: An LAC router running VPDN may crash when it receives an invalid redirect from its peer. The `SSS Manager Disconnected Session` CDN error message is displayed.

  Conditions: This issue is observed when the LAC router receives the following incorrect message from its multihop peer:

  ```
  Error code(9): Try another directed and Optional msg: SSS Manager   disconnected
  session <<<< INVALID
  ```

  Workaround: There is no workaround.

- CSCtj89941

  Symptom: The router crashes when the **clear crypto session** command is used on an EzVPN client.

  Conditions: This issue is observed when the **clear crypto session** command is used on an EzVPN client.

  Workaround: There is no workaround.

- CSCtj94141

  Symptom: A memory leak occurs.

  Conditions: This symptom is observed while creating an SLA MPLS probe through SNMP.

  Workaround: Use the CLI to configure the SLA MPLS operation.

- CSCtj94555

  Symptom: After a router is reloaded, it is not able to re-register with the KS.

  Conditions: This issue is observed on a router running Cisco IOS 15.0(1)S1.

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

- CSCtj96915

  Symptom: The LNS router stops responding at the interrupt level.

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

  Workaround: There is no workaround.

- CSCtk00976

  Symptom: The file descriptor reaches its maximum threshold limit. The `File table overflow` error message is displayed, and you cannot save the configuration or perform a file-system-related operation.

  Conditions: This issue is observed when the **dir/recursive <>** command is run multiple times by using the ANA tool.

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

- CSCtk02647

  Symptom: On an LNS router configured for L2TP aggregation, per-user ACLs downloaded through RADIUS may cause PPP negotiation failures (that is, IPCP may get blocked).

Conditions: This issue is observed when an LNS multilink is configured and negotiated for PPP/L2TP sessions and per-user ACL is downloaded for PPP users through RADIUS.

Workaround: There is no workaround.

- CSCtk12252

  Symptom: After the router is reloaded, a Priority 1, valid SONET controller network clock source is not selected as the active clock source. Instead, the clock remains in the FREERUN state.

  Conditions: This issue is observed after the router is reloaded, when there is a Priority 2 network clock source in the Valid But Not Present state.

  Workaround: Shut down and restart the near-end Priority 1 clock source SONET controller.

- CSCtk12608

  Symptom: Route watch does not notify the client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

  Conditions: This issue is observed when a RIB resolution loop changes.

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

- CSCtk12708

  Symptom: The router crashes when the holdover clock source is deleted.

  Conditions: This issue is observed when the holdover clock source is deleted.

  Workaround: There is no workaround.

- CSCtk30807

  Symptom: A router that acts as a DHCP relay or server crashes when the DHCP service is stopped and then started.

  Conditions: This issue is observed when the router is also configured as the ISG.

  Workaround: There is no workaround.

- CSCtk35953

  Symptom: Dampening information is not removed even when the dampening configuration is removed in VPNv4 AF.

  Conditions: This issue is observed when DUT has an eBGP-VPNv4 session with a peer and a same-RD import occurs on the DUT for the route learned from the VPNv4 peer.

  Workaround: Perform a hard reset of the session to remove the dampening information.

- CSCtk36582

  Symptom: The Acct-On and Acct-Off signals from the AZR clears all the sessions in the client pool.

  Conditions: This issue is observed in scenarios similar to the following sample scenario:

  There are two AZRs, 192.168.100.1 and 192.168.100.2. The client in the ISG is configured under the RADIUS proxy as follows:

  client 192.168.0.0 255.255.0.0

  When Acct-on and Acct-off signals are received from one of the clients, sessions on both clients are cleared.

  Workaround: Configure clients one at a time instead of configuring the entire pool.

- CSCtk47891

  Symptom: If FRR is configured, traffic may be lost when the LC is reset.

Conditions: This issue is observed when FRR is configured and is in the Active state when the LC is reset.

Workaround: There is no workaround.

- CSCtk53463

  Symptom: While running the **shape average** *cir_value bc_value* command, *bc_value* is limited to 4 milliseconds times *cir_value*. Here, 4 milliseconds is the minimum interval between bursts. However, the ES LC can support intervals that are smaller than 4 milliseconds. This is not the expected behavior for the ES LC.

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

  Workaround: There is no workaround.

- CSCtk67658

  Symptom: After an SSO is performed, traceback may be observed and the newly active RP may crash.

  Conditions: This issue is observed after an SSO is performed.

  Workaround: There is no workaround.

- CSCtk67768

  Symptom: The RP crashes during the DHCPD Receive process.

  Conditions: This issue is observed when a DHCP server is configured.

  Workaround: There is no workaround.

- CSCtk74970

  Symptom: A tunnel that is announced by the TE autoroute is not installed in the routing table.

  Conditions: This issue is observed when you first configure and remove one hop and LDP from the TE, and then configure one hop on the TE (without LDP).

  Workaround: Run the no ip routing protocol purge interface command.

- CSCtk75389

  Symptom: The PFR fallback interface does not stay in-policy.

  Conditions: The issue is observed when an ATM interface is used.

  Workaround: There is no workaround.

- CSCtl00127

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

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

  Workaround: There is no workaround.

- CSCtl04285

  Symptom: The BGP route reflector does not advertise new IPv4 MDT routes to PEs.

  Conditions: This issue is observed after a BGP session flap or while provisioning a new session.

  Workaround: Run the **clear ip bgp *** command.

- CSCtl08014

  Symptom: The router crashes and memory corruption symptoms are observed.

Conditions: This issue is observed when SSO or OIR is performed while MLP sessions are getting initiated.

Workaround: There is no workaround.

- CSCtl08601

  Symptom: When the DHCP pool is removed, the console stops responding.

  Conditions: This issue is observed when the **no service dhcp** command is run before the DHCP pool is removed.

  Workaround: There is no workaround.

- CSCtl21884

  Symptom: When autosummary is enabled under the BGP process, a **BGP withdraw** update is not sent even though the static route becomes unavailable.

  Conditions: This issue is observed when autosummary is enabled under the BGP process and a static route is brought into the BGP table by running the **network** command.

  Workaround: Under the BGP process, run the **clear ip bgp *** command or disable autosummary.

- CSCtl42358

  Symptom: The router crashes after the **no atm sonet overhead j1** command is run on an ATM interface.

  Conditions: This issue is observed after the **no atm sonet overhead j1** command is run on an ATM interface.

  Workaround: There is no workaround.

- CSCtl54033

  Symptom: After a sub-LSP is pruned or torn down, resignaling sub-LSPs for P2MP TE tunnels may require up to 10 seconds.

  Conditions: This issue is observed when a P2MP TE tunnel is configured to request FRR protection but no backup tunnel is available at the failure point to protect the sub-LSP.

  Workaround: Configure FRR backup tunnels at each node to provide link protection for P2MP TE tunnels.

- CSCtl67195

  Symptom: The following BGP debug commands cannot be used:

  debug ip bgp vpnv4 unicast

  debug ip bgp vpnv6 unicast

  debug ip bgp ipv6 unicast

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

  Workaround: There is no workaround.

- CSCtl83053

  Symptom: The shaper rate cannot be changed with ANCP Port Up messages.

  Conditions: This issue is observed when QoS and ANCP are enabled.

  Workaround: There is no workaround.

- CSCtl83736

Symptom: Each V4 session setup leaks approximately 100 bytes. Similarly, each V6 session setup leaks approximately 112 bytes.

Conditions: This issue is observed on IP sessions.

Workaround: There is no workaround.

- CSCtl88066

  Symptom: The router is automatically reloaded.

  Conditions: This issue is observed when BGP is configured and one of the following commands is run:

  show ip bgp all attr nexthop

  show ip bgp all attr nexthop rib-filter

  Workaround: Do not run either of these commands with the **all** keyword. Instead, run the address-family-specific version of the command for the address family.

- CSCtn01832

  Symptom: The router crashes when the following command is run:

  config check syntax route-map hello match local-preference no match local-preference

  Conditions: This issue is observed when the command mentioned in the Symptom description is run.

  Workaround: There is no workaround.

- CSCtn03930

  Symptom: A system error may be logged.

  Conditions: This issue is observed when RP switchover takes place while traffic is running on a router that functions as an IPSec termination and aggregation router.

  Workaround: There is no workaround.

- CSCto88686

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

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

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

Open Caveats—Cisco IOS XE Release 3.1.2S

This section documents possible unexpected behavior by Cisco IOS XE Release 3.1.2S

- CSCsa79984

  When using the line subcommand **login**, it may be possible for a vty to get into a state where the user will not be able to log in to the IOS router. The user will be presented with password followed immediately by “Bad passwords”.

  The line in this state can be seen with the exec command **show line <*line number*>**. In the “Status line**”**, if ‘Ctrl-c Enabled’ appears, then you may see this problem on that line.

Workaround: To clear this condition follow these sequence of steps:

1. First remove the login from the line.
2. Telnet into the router on the line which is in this state. From enable mode, run the command **setup**.
3. When prompted with “Continue with configuration dialog” type no.
4. Add the login back to the vty line.

- CSCtf84408

  Burst remove TP might cause iosd Segmentation fault(11) at Tunnel Security process.

  This condition is observed when using interface range command to remove TP from tunnel interface.

  Workaround: There is no workaround.

- CSCth11310

  IP-subscriber sessions stop forwarding traffic after RADIUS proxy resets them. The session does not appear to get any traffic, and drops may be observed when the following command is used:

  show platform hardware qfp active statistics drop

  This behavior may occur on ASR 1000 Router Series, with routed IP-subscriber sessions that are reset and converted to RADIUS proxy sessions.

  Workaround: There is no workaround.

- CSCth12830

  CE to CE ping fails on SSO switchover with L2TPv3 configuration on ATM interface.

  This condition has been observed when CE to CE ping fails on SSO switchover with L2TPv3 configuration on ATM interface with VP mode.

  Workaround: Is issue the **clear xconnect all** command.

- CSCth22250

  On 2RU-F and ESP-5 when bringing up translations at higher rate, all sessions cannot be established with high setup rate.

  Workaround: Lower the setup rate.

- CSCth74294

  On the ASR 1000 Router “stop” accounting message is seen on the router console for Acct-Input-Octets missing field:

  Acct-Output-Octets, Acct-Input-Packets, Acct-Output-Packets

  This condition is observed in DVTI- EzVPN topology during session tear down while the EzVPN server sends out accounting information.

  Workaround: There is no workaround.

- CSCti40325

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

  This symptom is seen when the RADIUS server is used for AAA.

  Workaround: There is no workaround.

- CSCtj05670

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

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

  Workaround: There is no workaround.

- CSCtj15181

  SMAND may not initiate when issuing **show policy-map type inspect zone-pair session** command.

  Workaround: Use HSL for retrieving **zone-pair** information.

- CSCtj16111

  ESP may not initiate on the Cisco ASR 1000 Router. This condition is seen when the router is configured as an ISG gateway, and has periodic L4 redirection configured for user sessions.

  Workaround: If the periodic redirection is not configured then the crash is avoided.

- CSCtj23259

  When the ASR 1000 Router acts as a PE and has scaled configs for L2TPv3 feature combination with EoMPLS and ATMoMPLS with 2000 pseudowires. A CC failure is observed when initiating CC OIR.

  This condition may occur when initiating CC OIR and the CC failure is observed. This may only happen when SIP has been configured with SPA-1XCHOC12/DS0's and SPA-2XOC3-POSs. This condition is not observed with any other SPAs.

  Workaround: There is no workaround.

- CSCtj31267

  IPv4 Multicast NAT traffic might create dynamic NAT 1 to 1 binding even when the traffic flow is not into out, or out to in on the ASR 1000 Router.

  Workaround: There is no workaround.

- CSCtj62999

  PPP sessions are not able to activate on the ASR 1000 Series Router.

  This condition is observed when PBR is configured under Virtual-template interface.

  Workaround: There is no workaround.

- CSCtj73536

  Traffic may stop when forwarding over to PPP Users, after PPP Users have been terminated on the Cisco ASR 1000 Router with L2TP Tunnel configured.

  This condition is observed when flapping occurs on the virtual-access interface, several times.

  Workaround: There is no workaround.

- CSCtj74404

  PEM status is not updating correctly even though one of the redundant PEMs are switched off (PEM status is still ok).

  This condition is observed when initiating the following:

  - After power cycle, or reload has occurred. If PEM status does not appear right after bootup, you may not see it's next power cycle
  - When using Cisco IOS XE 3.1.xS

Workaround: Reload or power cycle the box again.

- CSCtj80468

  ASR 1000 Series Router ESP-20 may experience failures during high sustainable churning, per-subscriber and Zone-based Firewall Stateful sessions after throughput has high PPP subscriber sessions churning.

  This condition is observed when the ASR 1000 Series Router is configured as an LNS, has ~15000 PPP subscribers in the Zone-based firewall with heavy stateful traffic, ~15000 PPP subscriber not having their traffic inspected, and there are numerous other subscriber churning activities. This has been observed in an MPLS environment, as well. If Aggregate traffic is between 7-10Gb's.

  Workaround: Is to back off traffic load and churn.

- CSCtj88724

  Standby ESP fails to activate and Traceback is thrown on the console after unconfiguring the interface while Broadband sessions are still up.

  This condition is observed when unconfiguring the Interface while Broadband sessions are still up on the router causing Standby ESP fails to activate and traceback is thrown on the console. In addition this failure, or traceback is not affecting the basic functionality of the router.

  Workaround: Stand by ESP failure is not always seen and since active ESP is always up, there is no interruption for service.

- CSCtj94131

  Only on the ASR 1002 Router the parse configuration time (is 5 seconds) may take too long.

  Workaround: There is no workaround.

- 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

Resolved Caveats—Cisco IOS XE Release 3.1.2S

All the caveats listed in this section are resolved in Cisco IOS XE Release 3.1.2S

- CSCsj78195

  Cisco IOS NAT CLI allows route-maps to be configured when defining static network translations.

Due to the current implementation of NAT and route-maps the use of route-maps with a static network translation is currently not supported. Therefore the CLI should block this configuration.

Workaround: There is no workaround.

- CSCsm98756

  CPU utilization peaks at 99% for a sustained period and various control plane functions such as SBC call setup may not function as expected. The symptom is observed with a large scale configuration (thousands of VLANs) and when performing the **show run | inc ipv6 route** command.

  Workaround: There is no workaround.

- CSCso09886

  When the **show zone security** and **show zone-pair security** commands are executed on the Cisco ASR 1000 Series Router, the console terminal spews all configured zones and zone-pairs. This condition occurs when the number of zones and zone-pairs configured exceeds the terminal length value.

  Workaround: There are no known workarounds.

- CSCsq70140

  The following error messages may seen may be seen on Cisco ASR 1002 and Cisco ASR 1004:

  No memory available: Update of NVRAM config failed!

  This happens more frequently when user are saving a very big configuration such as one with 16K interfaces on a ASR 1002 or ASR 1004. This problem is not seen on Cisco ASR 1006.

  Workaround: There is no workaround.

- CSCsq73935

  Invalid instance “0” is getting populated for tabular objects in dsx3ConfigTable. This issue is observed when configuring sonet framing on 1xCHSTM1/OC3-SPA, after the mode is set to “ct3” or “ct3-e1”and the “0” instances gets populated for the tabular objects.

  Workaround: This instance may be seen, when configuring any channelization on top:

  ```
  controller sonet 0/3/0
  sts1-1
  mode ct3
  ```

  Note If the mode is set to “ct3” or “ct3-e1”, the “0” instances are not returned

- CSCsq91659

  When a 1xCHSTM-OC3 SPA on the Cisco ASR 1000 Series Router is configured in unframed E1 mode and the SPA is reloaded using the **hw-module** *subslot* **reload** command, dsx1LineStatus returns an invalid value of “0.”

  There are no known workarounds.

- CSCsr50040

  If you disable **aaa policy interface-config allow-subinterface** on the Cisco ASR 1000 Router on a subinterface that has RADIUS attributes (such as an lcp:interface-config) creating full virtual access for broadband access (BBA) sessions, the system may report error messages and tracebacks.

  Workaround: Configure **aaa policy interface-config allow-subinterface** locally on the router.

- CSCsr87974

When the online insertion and removal (OIR) of a SIP is performed on a Cisco ASR 1000 Router, traceback occurs at fibidb_configure_lc_ipfib. No functional impact is observed.

Workaround: There are no known workarounds.

- CSCsr90264

  When Per-subscriber firewall PPPoX calls may not initiate, **Zoning is currently not configured for interface Virtual-Access** logs might appear.

  This condition is observed when Per-subscriber firewall is configured in a PPPoE environment. The involved virtual-template(s) contain a zone security statement placing the virtual-template in a zone. This zone is part of a valid zone-pair configuration and working service policy for that zone-pair. RADIUS authentication is used and the subject subscriber will download the same zone statement in their user profile as is described in the virtual-template to which this subscriber is being applied.

  For example: **lcp:interface-config=zone-member security zone_name**.

  The subscriber may not initiate its call attempt and router logs will include **Zoning is currently not configured for interface Virtual-Access**.

  Workaround: Use a different zone name belonging to a zone-pair with the same service policy as intended in the failing example above. Make sure **aaa policy interface-config allow-subinterface** is configured and not doing the analogous **lcp:interface-config=allow-subinterface=yes** via RADIUS in addition or concurrently.

  Further Problem Description: If what otherwise looks to be a valid config, enable vtemplate debugging (cloning, error, and subinterface at a minimum). The **lcp:interface-config** provisions the session as if you'd type the commands through the parser. The parser may return error messages, when such messages are detected, SSS assumes in the config manager that something went wrong and that results in a disconnect:

  ```
  *Aug 10 03:35:03.873: VT:Messages from (un)cloning Vi2.1:
  % Interface is already member of zone fw_low_zone *Aug 10 03:35:03.874: SSM CM: Query
  Lterm to L2TP switching, enabled
  And that results eventually in :
  *Aug 10 03:35:03.894: VT[Vi2.1]:Processing vaccess response, id 0x41D3D6C8, result
  clone error (4) *Aug 10 03:35:03.894: SSS MGR [uid:2]: Event feature-failed, state
  changed from installing-config to disconnecting-all
  ```

  This feature does not get reapplied, it throws an error message and that is when the session disconnects.

- CSCsu38228

  On a Cisco ASR 1000 Series Router with Weighted Random Early Detection (WRED) enabled, when **random-detect exponential-weighting-constant** is reset with valid values (1-6, default is 4) and removed from the policy map applied, the **random-detect exponential-weighting-constant** is set to 9.

  Workaround: Reconfigure **random-detect exponential-weighting-constant** to the correct value.

- CSCsv29870

  RIP sends multiple request after doing **clear ip route *** and interface state transitions.

  This condition is observed when RIP is configured and issuing **clear ip route *** afterwards RIP sends a multiple request for each interface instead of sending one request. This will cause the processing load on the request receiving side.

  Workaround: There is no workaround.

- CSCsx13031

The Route Processor (RP) on a Cisco ASR 1000 Series Router may reload unexpectedly shortly after switchover.

This condition is observed when the redundancy force-switchover command is executed immediately (within seconds) after the system reaches Stateful Switchover (SSO) mode.

Workaround: There are no known workarounds.

- CSCsx56362

  BGP selects paths which are not the oldest paths for multipath on a Cisco ASR 1000 Router. This causes BGP to unnecessarily flap from multipath to non-multipath as a result of route flaps.

  This condition has been observed when initiating the following:

  1. BGP is configured
  2. More than one equally-good route is available
  3. BGP is configured to use less than the maximum available number of multipaths

  Workaround: There is no workaround.

- CSCsy31159

  When the **show history all** command is executed on a Cisco ASR 1000 Series Router, the command does not immediately reflect all commands entered.

  Workaround: There are no known workarounds.

- CSCsy49927

  The IOSd restart is seen with crest proc frame that fetches the tcl shell for execution.

  This is seen with crest proc that helps in configuring a scale configuration.

  Workaround: There is no workaround.

- CSCsy85400

  The first VIA field in a Session Initiation Protocol (SIP) INVITE/BYE call is not getting properly translated by Network Address Translation (NAT). The NAT inside IP address is replaced by some invalid characters. Calls are NOT impacted due to this issue.

  This condition happens when no existing NAT translation for the session exists.

  Workaround: There are no known workarounds.

- CSCsy88034

  The “active” and “individual flow data” in the **show ip cache** [**verbose**] **flow** command output intermittently fails on a Cisco ASR 1000 Series Router. At times the “active” stat is zero, and at other times the individual flow data is missing.

  This problem occurs with very large configurations.

  Workaround: Reload the router.

- CSCsz37418

  There is no NHS entry on the HUB in SNMP tree.

  This condition is observed when the images are unable to initiate to create a Server entry on the HUB after some events.

  For example, the following events are seen:

  If the tunnel is configured after doing a **shut/no shut**, when the spoke has re-registered and verified by viewing the syslog messages the images are unable to initiate to create a Server entry on the HUB.

Workaround: There is no workaround.

- CSCsz53438

  On the Cisco ASR 1000 Series Router, if IP header compression is configured on the router, but not on the corresponding router, an unexpected reload of the embedded systems processor may occur.

  This condition may occur when IPHC is configured on the ASR 1000 Series Router, but not on the router to which it is directly connected to.

  Workaround: Is to **enable** IPHC on both routers.

- CSCsz56462

  When configuring cdp run it does not bring up cdp on the interfaces. This Conditions happens only if the default behavior of a platform is to have CDP disabled.

  Workaround: To enable CDP, include the cdp enable command in the configuration.

- CSCsz56462

  When configuring **cdp run** it does not bring up Cisco Discovery Protocol (CDP) on the interfaces.

  This conditions happens only if the default behavior of a platform is to have CDP **disabled**.

  Workaround: To **enable** CDP, include the **cdp enable** command in the configuration.

- CSCsz82080

  An Cisco ASR 1000 Router may not activate with ESP when an IPSec Tunnel is removed or modified.

  Workaround: When modifying or removing a tunnel interface remove the IPSec command first. After the change has been made IPSec can then be applied again.

- CSCta31582

  The netflow export command **ip flow-export version 9 bgp-nexthop** by itself has no effect meaning no BGP nexthop information is placed into the Netflow cache or records as a result of the bgp-nexthop token. If instead the commmands <CmdBold> **ip flow-export version 9 origin-as bgp-nexthop** or i**p flow-export version 9 origin-as** are issued, then BGP nexthop information is included in all cases.

  This instance can occur on any ASR 1000 Router platform running the NetFlow feature.

  Workaround: The workaround is covered in the above description. If BGP Nexthop info is desired configure either *origin-as* or *peer-as* in the exporter command and this will cause BGP Nexthop information to appear in the cache and the export records.

- CSCta43825

  A CMTS walk of the ARP table causes high CPU usage.

  This symptom is also seen with an SNMP walk of the ARP table.

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

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

- CSCta65347

  There is no media after resuming the call on the ASR 1000 Router Series. Only in this instance the resume fails, when CCM/CME scenario's from h323 legcalls are used.

Workaround: There is no workaround.

- CSCta69213

  When the Cisco ASR 1000 Series Router is configured for NHRP it may not activate due to a bus error.

  This symptom is observed on a Cisco ASR 1000 Router configured for NHRP and DMVPN.

  Workaround: There is no workaround

- CSCtb24959

  The ASR 1000 Router may fail while clearing large number of rp mappings.

  This instance can happen when the following has occurred:

  1. The router has been configured for RP agent
  2. and candidate there are a large number of RPs.
  3. When initiating the **clear ip pim rp-map** command
  4. a failure has been observed on the router.

  Workaround: Is not to apply the **clear ip pim rp-map** command one after the other.

- CSCtb32892

  Traceback has been logged **%MFIB-3-DECAP_OCE_CREATION_FAILED: Decap OCE creation failed** may be seen on the ASR 1000 Router Series console when loading the image or adding the RP with SSO.

  In this condition, the tracebacks can be seen on reloading a Provider Edge router with mVPN configuration or adding the RP with SSO on the router.

  Workaround: There is no workaround.

- CSCtb33587

  NDB state Error Tracebacks on DMVPN spoke with NHO may be found on the ASR 1000 Router Series:

  ```
  %IPRT-3-NDB_STATE_ERROR: NDB state error (NO NEXT HOPS UNEXPECTED)
  ```

  This may cause temporary packet drops or forwarding to less specific routes.

  The problem may occur, when using RIP or EIGRP and running NHRP and NHRP has installed NHO nexthops for the RIP/EIGRP route.

  Workaround: Is to wait after the holddown timer expires, the problem will be cleared.

- CSCtb79598

  When you configure a PVC ASR 1000 with QoS enabled, the QoS will not work as expected on the ASR 1000 Router Series.

  The only happens, when you unconfigure **ancp neighbor** associated with the PVC before you delete the PVC on the ASR 1000 Router.

  Workaround: There is no workaround.

- CSCtb84718

  Output of show cli **"sh crypto gdoi gm acl"** does not correctly display as a COOP Key Server.

  This has been observed, when COOP Key Servers has been configured on the GM.

  Workaround: There is no workaround.

- CSCtc19914

The Embedded Services Processor (ESP) has been reloaded when configuring and unconfigure a large static RP addresses multiple times rapidly with mVRFs on the ASR 1000 Router Series.

This condition has been seen when using the following scripts:

1. Configuring large mVRFs on PE
2. Configuring large loopbacks on PE, one for each of the VRF
3. Configuring and unconfiguring large static RP addresses multiple times rapidly.

Workaround: There is no workaround.

- CSCtc21042

  Chassis-manager process on RP2 gets stuck and the ASR 1000 Router becomes unresponsive to user commands. All the FPs and CCs keep rebooting, with console logs showing repeated FP code downloads.

  No particular scenario is known. This problem may caused by OBFL logging of messages on RP2.

  Workaround: Is to disable onboard logging of messages on RPs as shown in this following example:

  hw-module slot r0/r1 logging onbaord disable

```
Router#hw-module slot r0 logging onboard disable

To verify that onboard logging has been disabled:
 Router#sh logging onboard slot r0 status
 Status: Disabled
```

Note This command is not saved in the config so is not preserved across router reloads.

  Workaround: There is no workaround.

- CSCtc25791

  A router may not activate when issuing **show** commands related to EIGRP and routing information while the EIGRP configuration is being removed.

  This symptom is observed when EIGRP is configured when there are minimum of two users logged into the device issuing **show** commands.

  Workaround: Do not issue **show** commands regarding EIGRP or routing while removing the EIGRP configuration.

- CSCtc55049

  The ASR 1000 Router may not intiate and reload following a reboot or initial boot from a power-up.

  The embedded syslog manager (ESM) needs to be configured along with an ESM script present during an initial boot or reload. Also, redundant RP/FP appears to be the scenario that has the greatest likelihood of encountering the problem.

  Workaround: There is no workaround. However, if the problem manifests, the subsequent rebooting is very likely to be successful. When stuck in a situation where crashes are repetitive, momentarily pull redundant RP until system stabilizes, and re-insert redundant RP.

- CSCtc62440

  On a Cisco ASR 1000 Router Series, the removal of subinterfaces may under certain conditions result in MFIB_MRIB-3-FAILED_WIRE_FIND error messages being generated on the Route Processor (RP).

There is no functional impact due to this issue.

Workaround: There are no known workarounds.

- CSCtc72052

  The ASR 1000 Router is unable to configure Dynamic Nat Pool with prefix length 14 or less.

  This happens when Nat Pool is configured with a lower prefix lengths. This configuration is rejected on the ASR 1000 Router.

  Workaround: Is to create a Nat Pool with prefix length 14 or higher.

- CSCtc73525

  The ESP board on the ASR 1000 Router Series with ATM PVCs carrying broadband sessions does not accept further config. Traffic forwarding on existing features and session is not impacted, but additional config is rejected.

  This occurs when BB sessions over ATM PVCs are configured. With a high number of PVCs configured, and if all PVCs are attempted to be removed at once with the "rage" command, the ESP board may get into an error state that prevents additional config (such as bringing up new PVCs or sessions) from being accepted.

  Workaround: There is no workaround. However if problem manifests, a reload of the ESP is required to bring the system back to its normal state.

- CSCtd13999

  When an ASR 1000 Router is running IOS the router may pick an incorrect MSS when path-mtu is enabled. The incorrect MSS is lower than what the network path can support.

  This symptom is triggered when a transit router sends more than one ICMP-too-big messages.

  Workaround: There is no workaround.

- CSCtd14559

  L2TP-3-ILLEGAL tracebacks and PPPoX session mismatch between active and standby rps.

  This error condition is noticed, when rp switchover takes place during the time frame pppox sessions are coming up. In a rare condition, session mismatch was noticed when pppox sessions were coming up for the first time with no other events taking place.

  Workaround: There is no known workaround

- CSCtd21252

  Unified SBC crash has been seen on the ASR 1000 Router Series.

  This condition may occur, when configuring a large IPv6 media-address on the router.

  Workaround: There is no workaround.

- CSCtd32560

  During Cisco ASR 1002 or Cisco ASR 1004 ISSU upgrade from IOS XE 2.3.2 to IOS XE 2.5.0, a loss of QoS functionality can occur on some and all targets.

  Loss of QoS functionality has been observed right after RP upgrade and switchover while following Cisco ASR 1002 or Cisco ASR 1004 ISSU procedure. The QoS functionality does not recover on its own and only occurs on policies that are both hierarchical (at least 2-level) and contain policers. The condition can be identified by the following command:

  show platform hardware qfp active interface if-name <if_name> info | include QoS

  If there is no output returned from this command then there has likely been a QoS service disruption due to this problem.

Workaround: QoS functionality can be resumed on the interface by removing and re-attaching the QoS policy. Alternately, the problem can be avoided by upgrading to IOS XE 2.4.x first (including the ESP). The upgrade path would be IOS XE2.3.2 -> IOS XE 2.4.x -> IOS XE 2.5.x.

- CSCte09945

  When an Cisco ASR 1000 Router operates in the Unified SBC mode, after a hardware switch over using CLI **redundancy force-switchover**, during the old active RP is booting, issue CLI **no sbc**. Check failure error is observed in the RP console log.

  Workaround: No workaround until now.

- CSCte14955

  A Cisco ASR 1000 Series Aggregation Services router may experience an unexpected reload.

  The symptom may occur when multiple tunnel interfaces are configured with **mpls bgp forwarding**, if the tunnel interfaces are flapping.

  Workaround: Configure the eBGP sessions on interfaces other than tunnel interfaces.

- CSCte17127

  Calls are failing due to an invalid tls certificate or they may be completing when the certificate is invalid.

  This issue ties into how long the SBC keeps the tcp and tls connection up and also when the ASR 1000 Router does not revalidate the certificates for a deleted or newly added trust point tls peer. The same applies to the scenario where a certificate has to be replaced.

  Workaround: Set the tls idle timer to a value of 3 minutes to minimize the time that the tls peer. This will cause the ASR 1000 Router to revalidate the certificate. Another option is to use the **show tcp brief** command to find the peer connections and then use the **clear tcp brief tcb XXXXX** to clear the existing connections. This will cause the ASR 1000 Router to revalidate the peer.

- CSCte61735

  Memory leak has been seen when MQC is configured on the Cisco ASR 1000 Router.

  This can occur, when QoS has been configured on the router, in an ISG environment.

  For example the following conditions have been observed:

```
interface ATM4/0.1 point-to-point
no atm enable-ilmi-trap
pvc 0/101
class-vc crosshairs
vbr-nrt 500 400 50
dbs enable
service-policy in DefaultIn
service-policy out DefaultOut
 !
vc-class atm crosshairs
protocol ppp Virtual-Template1
encapsulation aal5snap

interface Virtual-Template1
ip unnumbered Loopback0
ppp authentication chap
end
```

  The memory leak occurs when a link is flapped up and down.

  Workaround: There is no workaround.

- CSCte78406

On the Cisco ASR 1000 Router console the following error message has been logged on the new standby RP, when PTA sessions are established:

*Feb 2 10:21:36.635: %COMMON_FIB-3-FIBIDBINCONS2: An internal software error occurred. Virtual-Access2.1 linked to wrong idb Virtual-Access2.1

This condition may occur, once PTA sessions are established when performing a RP switchover. After both RPs are synced up with flapped sessions. The error messages are logged on the new standby RP.

Workaround: There is no workaround.

- CSCte78938

  Xconnect configuration is rejected after replacing the MPLS xconnect configuration with manual L2TPv3 configuration on the ASR 1000 Router Series.

  This condition has been seen, when EoMPLS xconnect is configured, while trying to modify the configuration to use L2TPv3 Xconnect on the router.

  Workaround: Do not configure L2TPv3 on an interface which previously was used for EoMPLS.

- CSCte82240

  SBC accepts "." when key_addr_type is "DIALED_DIGITS". This condition can occur, when set exact matching means has been set as:

  rpsRtgActionKeyAddrWildcardType to AMB_MW_EXPLICIT_WILDCARD.

  This is possible to have a "." when rpsRtgActionKeyAddrType is set to AMB_MW_ADDR_TYPE_DIALED_DIGITS. However, it is no longer allowed when rpsRtgActionKeyAddrWildcardType is AMB_MW_EXPLICIT_WCARD (which means SBC should perform an explicit match).

  Workaround: There is no workaround.

- CSCte83888

  When PoD request contains target Acct-Session-Id prepended with NAS-Port-ID

  it will not be honored.

  This condition has been observed, when PoD prepended is configured with NAS-Port-Id for target sessions.

  Workaround: Is to use only the Session-Id which is located after the, "_" in the Account-Session-ID

  to specify the session needing disconnect.

- CSCte95396

  A subscriber cannot enable the SSS session due to DPM not finding the binding in the DPM table although the DHCP binding exists as shown by performing the **show ip dhcp server binding** command.

  Debug sss policy event/err would show **SG-DPM: DHCP Binding does not exist query session**.

  This conditions is observed when doing the following steps:

  - Subscriber has dhcp binding after initiating **show ip binding ...**

    note: also check the vrf (if any).

  - Subscriber has no entry in the dpm policy.

  - Session trigger needs to be l2-connect dhcp

  Workaround:

-If this is a “slow lease time and relay dhcp case", make sure subscriber does not send a DHCP packet:

waiting for the DHCP binding to disappear (i.e., expire), re-enable the user's dhcp forwarding path.

-If this is a “dhcp server”case, clear dhcp binding on the ISG.

-Reload the router

- CSCte97907

  On a Cisco ASR 1000 Router (RP2) may get out of sync with NTP master every 18 minutes for approximately 1 minute. This may offset the NTP Master which will cause an increase up to -1052.1 msec and the sync will get lost.

  This instance has been observed, when NTP is enabled and running apr. 20 minutes.

  Workaround: There is no workaround.

- CSCtf01618

  A Cisco ASR 1000 Series Aggregation Services router may unexpectedly reload due to SegV error.

  The symptom is observed when the router is running Cisco IOS Release 12.2(33)XND1, or later XND, or later 12.2(33)XN, and running DMVPN with tunnel protection.

  Workaround: Move to an unaffected release or remove tunnel protection.

- CSCtf04257

  On a Cisco ASR 1000 running IOS XE 12.2(33)XND1 below message may be seen, when trying to configure a EoMPLSoGRE VC:

  %SW_MGR-3-CM_ERROR: Connection Manager Error - provision segment failed [SSS:Eth:<number>] - no resources available.

  This condition has been seen on Cisco ASR 1000 Router, running IOS XE 12.2(33)XND1 and under the following conditions:

  – When destination of VC is changed from original to something else and then changed back to original
  – This happens only if we do not exit xconnect submode after the first change and proceed immediately to the second change, then exit via ^Z. The problem does not occur if we exit xconnect submode after the first change.

  Workaround: There is no workaround. If the problem has already occurred, you will need to reload. However, to avoid the problem, exit the config after each change. Do not repeat the same change in the xconenct submode back to back.

- CSCtf05408

  IP address on a loopback interface is lost on the Cisco ASR 1000 Router Series.

  Workaround: Is to reconfigure the loopback interface.

- CSCtf69128

  CRL cache size increases in the multiple of 1024 after each reload

  This condition is observed after configuring the CRL parsed cached size using **crypto ca crl cache size**, the show command:

  (show crypto pki crls) will show an incorrect cache size.

  Workaround: There is no workaround.

- CSCtg13269

On peers of Route Reflectors (RR), the received prefixes counter shows an incorrect number when session flaps occur during a network churn.

The symptom is observed with BGP on peers of Route Reflectors (RR's) configured on the ASR 1000 Router.

Workaround: Use the **clear ip bgp *** command.

- CSCtg35130

  EIGRP does not come up on a serial interface, on an ASR 1000 Router after reload.

  This behavior is seen, when a serial interface that is part of a VRF after the serial interface is configured with PPP and IP Unnumbered loopback commands, while the interface is part of EIGRP.

  Workaround: The following resolves the issue:

  1)enter **no ip unnumbered loopback** command.

  2)again enter **ip unnumbered loopback** command

- CSCtg53307

  The QoS police functionality might fail if user configures both “police” and “priority <kbps>” in the same traffic class.

  This behavior is observed when user configures this unsupported configuration with “police” and “priority <kbps>” in the same traffic class, actually only one police feature is supported per traffic class, and later remove one of the commands, the traffic sent through this class might fail to be policed to the configured rate.

  Workaround: Only enable one police feature in the same traffic class.

- CSCtg53307

  The QoS police functionality might fail if user configures both “police” and “priority <kbps>” in the same traffic class. This condition may occur when the user configures this unsupported configuration with “police” and “priority <kbps>” in the same traffic class, actually only one police feature is supported per traffic class, and later remove one of the commands, the traffic sent through this class might fail to be policed to the configured rate.

  Workaround: Is to only, enable one police feature in the same traffic class.

- CSCth24984

  High CPU usage on when RP1 is configured as DMVPN HuB. This condition may occur when having 1000 Static BGP neighbors(Spokes) over DMVPN Hub.

  Workaround: There is no workaround.

- CSCth27728

  After SBC has been configured on an ASR 1000 Router, and a SIP call is made. The router reloads.

  This condition has been seen when the **del-prefix 0** instructs SBC to remove the first zero digits from a dialed number, which means not doing anything. SBC does not handle being instructed to remove zero digits from the number and this is may cause a failure. Removing this from the config should result in the same behavior and may avoid the router to fail.

  Workaround: By removing **edit del-prefix 0 add-prefix 64** from the config and replacing it with **edit del-prefix 1 add-prefix 64** this should prevent the router from failing.

- CSCth41121

  An ASR 1000 Router may reload while processing a renegotiation rejection (reINVITE 491) on a call which is being transcoded. This condition occurs when a reINVITE is rejected (a renegotiation failure) on a call which is already established and not using a transcoder. The reINVITE was

attempting to use a transcoder (the new stream needed transcoding). The trigger for this failure is that the renegotiation adds an extra stream to the call (a new m= line in the SDP) and the reINVITE is rejected.

Workaround: There is no workaround.

- CSCth46888

  When the ARP entry is refreshed due to timeout or use of the **clear arp** command, the router sends ARP request for cached MAC address. However, the request message does not use virtual MAC for Source (Sender) MAC.

  The symptom is observed when the router is VRRP master and VRRP IP is configured the same as the interface IP.

  Workaround: There is no workaround.

- CSCth49844

  Cost extended BGP community is not handled properly on the ASR 1000 Series Router.

  This symptom is observed in the following environment:

  – Paths are received via eBGP.

  – Cost community is set via inbound route-map.

  Workaround: Use **bgp bestpath compare-routerid**.

- CSCth64122

  When using Lawful Intercept functionality in IOS and you use the cTap2MediationSrcInterface to the set source interface of IAP to MD traffic which is part of a VRF, the VRF's routing table will not be used, the global routing table will be used instead.

  Workaround: Is to have the source interface of IAP to MD traffic be in the global routing table, not a VRF, or set cTap2MediationSrcInterface to 0 to allow any interface to be used.

  In addition, to fix this behavior: Is to have the source interface updated properly if SNMP input interface object (cTap2MediationSrcInterface) mentioned above is valid. Hence, now the routing will happen using VRF routing table.

- CSCth68125

  SNMP MIBS counter for output/input packets/bytes such as ifOutOctets, ifHCOutOctets, ifHCOutUcastPkts and similar counters will not increment on multiple subinterface. After issuing **show vlan** counter command this will not allow for the increments to increase on an interface.

Note When a large number of subinterfaces are presented under the main interface, the stat update will take a longer time. This may take up to few secs or minutes based on number of subinterface configured with traffic in Cisco IOS XE Release 2.5.0.

This condition may persist when there are multiple subinterfaces configured and the main interface went into tunnel/L2-transport mode. The above condition has been seen on ASR 1000 Router Series.

Workaround: There is no workaround for Cisco IOS XE Release 2.5.0.

For Cisco IOS XE Release 2.6.0 and later releases: Configure ***hw-module subslot <> ethernet vlan unlimited***

Recovery: Is to perform **shut/no shut** on the main interface, if this condition still persist then reload the SPA.

Note The above workaround and recovery mechanism will impact traffic.

- CSCth83143

  IPv6 access list applied to SNMP community string does not work.

  This symptom is observed when an IPv6 ACL is applied to a SNMP Community string.

  Workaround: Is to do the following:

  1. Use SNMP Community string without an ACL.
  2. Use other means to block SNMP access to the device.

- CSCth83442

  When the ASR1002-F Router is functioned as a border router in Performance Routing (PfR) and the echo probes are created on the router, the ASR1002- F Router reloads while executing the **show ip sla statistics** or the **show ip sla configuration** commands.

  This condition has been observed when the PfR master controller has learn enabled, there are learn lists configured and the policy rule has not applied. The master controller has learned the prefixes from the border routers and has instructed the border routers to create the echo probes.

  The border router has learned the prefixes and echo probes are created and sent.

  Workaround: Do not execute the **show ip sla statistics** or **show ip sla configuration** commands.

- CSCth83464

  IPv6 route shows invalid subnet on RADIUS accounting packet.

  This behavior is observed when an IPv6 route statement is entered, the statement that shows up on the accounting server is not complete.

  Workaround: There is no workaround.

- CSCti01036

  On the Cisco ASR 1006 a failure may occur during RADIUS Process.

  This behavior is observed after an ASR 1000 Router with RADIUS AAA services is enabled. When the RADIUS server sends attributes with no information (empty VSA strings) it produces an unexpected reload on ASR 1000 Router.

  Workaround: Is to prevent AAA server from sending empty VSA strings.

- CSCti05663

  A DHCP ACK which is sent out in response to a renew gets dropped at relay.

  The symptom is observed in the case of an numbered relay.

  Workaround: There is no workaround.

- CSCti10518

  Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the rib.

  This condition has been observed when redistribution is occurring into EIGRP and the route ownership is changing in the middle of the redistribution process, EIGRP may leak the ndb in process.

  Workaround: There is no workaround.

- CSCti30149

  One of the case values in the EIGRP registry is corrupted. This is seen right after bootup.

This symptom is observed when some of the files are compiled with optimization.

Workaround: The corruption is not seen if the files are compiled with optimization **disabled**.

- CSCti35960

  IOS config relating to Persistnet Webui is not picked up during bootup.

  This condition is observed on an ASR 1000 Router with persistent webui config, while rebooting the router.

  Workaround: After boot up, you can render that lost config, and webui does start as usual.

- CSCti45810

  A router running Cisco IOS XE Release can experience processor memory leak with AAA enabled as well as SSH. A processes that is showing leaks with in the **show mem** allocating totals include "Dead" and "AAA General DB" processes.

  Another effect of this behavior is that the system failure may occur if an ssh session to the system is attempted while the system is low on memory.

  This condition is observed when SSH and AAA is **enabled**.Workaround: Change SSH session from password authentication to keyboard interactive authentication.

- CSCti48014

  A device reloads after executing the **show monitor event <comp> ... all detail** command (where ***<comp>*** is an option listed under **show monitor event ?**).

  This symptom is observed if the configurations are done in the order below:

  1. monitor event-trace ***<comp>*** stacktrace ***<depth>***
  2. monitor event-trace ***<comp>*** size ***<size value>***

  and any related event gets recorded in between the above two configurations.

  Workaround: To avoid this failure, change the order of the above configurations;

  that is, configure the "**size**" command first and then configure the "**stacktrace**" command.

- CSCti60740

  IOS failure may occur after the **disconnect** command is issued.

  This symptoms is observed when the router is accessed through multiple telnet sessions. There may be a chance after issuing **disconnect** command to a telnet session may result in a failure due to the time gap that exists while waiting for the user to hit enter to confirm if telnet session has ended.

  Workaround: Avoid using the **disconnect** command to disconnect a session.

  Alternative: An **exit** command can be used instead.

- CSCti63499

  A service policy stays in suspended mode.

  This condition only occurs occasionally after a reload or switchover.

  Workaround: Remove and re-apply the service policy to the interface.

- CSCti66076

  A standby HSRP router could be unknown after reloading the ES20 module that is configured for HSRP.

  This symptom is observed under the following conditions:

  – HSRP version 1 is the protocol that must be used.

- Use HSRP with subinterfaces on ES20 module
- Reload the ES20 module

Workaround: Change to HSRPv2, which is not exposed to the issue.

Alternate Workaround: Perform the following steps:

1. Reconfigure HSRP on all subinterfaces.
2. Configure multicast or igmp configuration on the interface where HSRP is configured (like ip pim sparse-mode)."

- CSCti74823

  Removing an address-family configuration while the prompt is in that address-family sub mode will cause the parser to return to the parent router prompt; however, the parser context values are still set to the address-family context.

  This occurs when issuing the command **no address-family vrf "name"** while in **address-family vrf "name"** configuration mode.

  Workaround: Exit out of the address-family configuration mode prior to deleting the address-family using the **exit**command and then **no address-family vrf name** command."

- CSCti81291

  This is no accounting-start sent by LNS.

  This condition is observed when AAA with accounting delayed-start, while LNS is configured for IPv4 *and* IPv6 on the virtual-template Client only negotiates IPv4.

  Workaround: There is no workaround. There is an optimal workaround when doing the following:

  - Remove ipv6 from vtemplate
  - Remove delayed-start
  - If the IP address is provided by RADIUS, you can remove the requirement for delayed-start by adding:

    ```
    > aaa accouting include auth-profile framed-ip-address
    > aaa accounting include auth-profile framed-ipv6-prefix
    > aaa accounting include auth-profile delegated-ipv6-prefix.
    ```

- CSCtj00039

  Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

  The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

  Workaround: Clear the route on the PE router using **clear ip route vrf<*xxx x.x.x.x*>**.

- CSCtj15805

  Keepalive functionality not working. An ICMP echo reply coming back from a client is ignored by ISG.

  The symptom is observed when a VRF mapping service is used.

  Workaround: There is no workaround.

- CSCtj46144

  After issuing the command **show platform** when PEM PRU is displayed on an ASR 1006 Router console: **2RU FM**

The symptoms are observed with the following steps:

1. After ASR1006-PWR-DC is removed.
2. Running 12.2(33)XNF2a

Workaround: There is no workaround.

- CSCtj48387

  After a few days of operation, an ASR 1000 Router running as an LNS box may not activate with DHCP related errors. The is behavior is observed when DHCP has been enabled and while sessions are receiving DHCP information from a RADIUS server.

  Workaround: There is no workaround.

- CSCtj49133

  After attaching a policy-map to a subinterface, the policy-map is then renamed and then the subinterface is deleted. The policy-map definition can not be deleted and still shows up in the running configuration.

  The symptoms are observed with the following steps:

  1. Attach a policy to a subinterface.
  2. Rename the policy-map.
  3. Remove the subinterface.
  4. Removing the definition of policy-map will not succeed.

  Workaround: Remove the service policy from subinterface before removing the subinterface.

- CSCtj56142

  ISG uses dummy user-name within EAP re-authentication related access-requests as the session dentifier. The symptom is observed during EAP re-authentications and likely after CoA-based service activation on an EAP-authenticated session. This happens only when the EAP access-requests carry a dummy user-name and access-

  accept does not have the correct username.

  Workaround: There is no workaround.

- CSCtj61252

  Router failure may occur when bringing up PPP sessions.

  The symptom is observed when adding QoS classes using parametrized QoS attributes where a class name to be added happens to be sub-string of an already existing class.

  Workaround: Do no add or configure class names which are sub-strings of other classes on the router.

- CSCtj73536

  Traffic will be stopped to forward to PPP users when PPP users has been terminated on an ASR 1000 Router with L2TP Tunnel configured.

  This behavior happens only when flapping has occurred on a virtual-access interface, several times.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.1.1S

This section documents possible unexpected behavior by Cisco IOS XE Release 3.1.1S

- CSCta31582

  The **ip flow-export version 9 bgp-nexthop** command by itself has no effect meaning no BGP nexthop information is placed into the Netflow cache or records as a result of the bgp-nexthop token. If instead the commands **ip flow-export version 9 origin-as bgp-nexthop** or i**p flow-export version 9 origin-as** are issued, then BGP nexthop information is included in all cases.

  This instance can occur on any ASR 1000 Router platform running the NetFlow feature.

  Workaround: The workaround is covered in the above description. If BGP Nexthop info is desired configure either *origin-as* or *peer-as* in the exporter command and this will cause BGP Nexthop information to appear in the cache and the export records.

- CSCte98201

  When **show network-clock** indicates a **valid** BITS clock state as **valid but not present** on the ASR 1000 Router Series.

  When a **valid** state BITS clock is removed and re-added in non-revertive mode, then **show network-clock** indicates BITS state as ***Valid but not present*** even though the Active Source indicates as BITS.

  Workaround: There is no workaround. This seems to be a display issue with the **show network-clock** cli output due to the fact that BITS is indicated as the Active Source.

- CSCtf01109

  The NAS-IP-Address value in the **accounting start** changes after an RP SSO. Before the RP SSO, the NAS-IP-Address contains the IP address of the interface connected to the AAA server. After an RP SSO, the new active RP sends out a new accounting start. This time, the NAS-IP-Address contains the loopback 0 IP address. When the session disconnects, the accounting stop record contains the correct IP address.

  The symptom is observed in a redundant RP system with PPP subscribers.

  Workaround: There is no workaround.

- CSCtf84146

  An interface may not be cleanly deleted on the ESP board, but is deleted in IOS on the RP.

  This can be detected via the following command (when run against a subinterface which has previously been deleted via IOS):

  router-6ru#sh plat hard qfp acti int if-name Tunnel10

  General interface information

  Interface Name: Tunnel10

  Interface state: VALID

  Platform interface handle: 30

  QFP interface handle: 25

  Rx uidb: 245748

  Tx uidb: 245735

  Channel: 0

  ...

  ...

  On an ASR 1000 Router Series the removal of subinterface with an FNF-NBAR configuration still attached may not cause the subinterface to be removed on the ESP.

Workaround: Remove the FNF-NBAR configuration before deleting the subinterface.

Once in the problem state:

1. config from qfp can be removed like this:

   a. create the interface again,

   b. attach same flow monitor,

   c. remove flow monitor,

   d. remove interface.

2. if the same flow monitor needs to be attached.

   a.create the interface again,

   b. attach same flow monitor,

   c. remove flow monitor,

   d. attach same flow monitor again.

3. Reload the ESP.

- CSCtg47777

  CPU utilization goes high while executing sh command with scaling configuration.

  This condition has been seen when scaling BFD with 128 peers configured on the router.

  Workaround: There is no workaround.

- CSCth42453

  SIP endpoints with shared line appearance fail to receive incoming call properly after an Cisco ASR 1000 Router failover.

  This instance has been observed when SBC CUBE(SP) is running on an ASR 1000 Router. There is no impact to normal SIP endpoint services.

  Workaround: There is no workaround.

- CSCth45402

  When configuring flow exporter VRF destination the port setting is ignored.

  This condition has been observed when a flow exporter has a destination VRF configured but the VRF does not exist.

  Workaround: Do not apply VRF configuration to flow exporter for VRFs that do not exist.

- CSCth47092

  Some classification related show commands could take long time to complete, when the configuration is large. The slowness of the show commands could make the system looks like halt. For an example, when executing **show tech** command.

  This condition has been observed when the configuration in device is large.

  Workaround: There is no workaround.

- CSCth50504

  The CUBE(SP) product reloads when configured with a large number of adjacencies, traffic is initiated, and then the entire SBC is deactivated with **no activate**.

  This condition has been observed when scaled configuration is under load.

  Workaround: Remove the traffic from the system before completely deactivating.

- CSCth54285

  Remark statement in IPv6 ACL creates a dummy ACE entry in the tcam.

  This instance can occur when presence of remark statement entry is in IPv6 ACL.

  Workaround: There is no affect on functionality.

- CSCth55640

  CE to CE ping failed over when EoMPLS is configured is configured in the native vlan interface

  This conditions has been observe when CE to CE ping failed after EoMPLS is configured in the native vlan interface.

  Workaround: This issue not seen while unlimiting the vlan range by using the CLI **hw-module subslot < > ethernet vlan unlimited**.

- CSCth68986

  Embedded Services Processor (ESP) may be reloaded. This condition may occur when executing a specific configuration sequence by adding and deleting **bandwidth** and **shape** command in the same traffic class, ESP might hit internal error and gets reloaded.

  Workaround: Remove QoS service-policy before modifying policy-map configuration, then reattach the service-policy back to interface.

- CSCth83070

  Invalid error message in the IOS log and there is no impact to the functionality. This condition may happen after enabling APS when running a few switchovers triggered by OIR. In addition after disabling APS and then enable it again may cause the error to occur.

  Workaround: There is no workaround.

- CSCth83442

  When the ASR1002-F Router is functioned as a border router in Performance Routing (PfR) and the echo probes are created on the router, the ASR1002- F Router reloads while executing the **show ip sla statistics** or the **show ip sla configuration** commands.

  This condition has been observed when the PfR master controller has learn enabled, there are learn lists configured and the policy rule has not applied. The master controller has learned the prefixes from the border routers and has instructed the border routers to create the echo probes. The border router has learned the prefixes and echo probes are created and sent.

  Workaround: Do not execute the **show ip sla statistics** or **show ip sla configuration** commands.

- CSCth89976

  Applying monitor with valid exporter and flow record to an interface does not take effect, **show flow exporter template** shows blank output.

  This condition may be seen when configuring FNF monitor on ASR 1000 Router with redundant RPs. The monitor should have a valid exporter and flow record with it. These config actions take place on the active RP. Now do a switch over. Apply monitor to an interface on the newly active RP, after switchover. The monitor may not be correctly applied to the interface.

  Workaround: Delete the flow record and monitor and re-apply.

- CSCth92727

  RTCP traffic in send_only mode is not policed to 5% of tman.

  This condition has been observed when an RTCP pinhole in send_only mode is established, and transmitted traffic has occurred.

Workaround: There is no workaround for this issue. The issue does not impact call rate or quality, but the flow stream will not be policed below the default rate for RTCP traffic.

- CSCth92832

  When a TE tunnel is shut down on a PE router traffic can still flow from the remote PE to the CE behind the shutdown TE tunnel.

  For an example:

  1. The tunnel is shut down on PE1.
  2. Traffic can still flow uni-directionally from CE2 to CE1.
  3. Traffic from CE1 will be dropped on ingress at PE1.

  This condition has been observed when EoMPLS is configured with MPLS signaling provided by a MPLS-TE tunnel.

  Workaround: Issue **clear xconnect all** on the remote PE after the TE tunnel is down to cause the remote PE to correctly drop traffic on ingress.

- CSCth96004

  BGP derived Netflow fields (Origin AS, Peer AS, BGP Nexthop) display incorrectly as zero when egress netflow is enabled on an interface in the case where the packets entered on the ASR 1000 Router as MPLS encapsulated packets and are exiting on an ASR 1000 Router as (non-MPLS) IPV4 packets.

  For example:

  Interface configuration for egress netflow can be either

  ip flow egress

  or

  mpls netflow egress

  To display the records in the Netflow cache the verbose form of the show command is used.

  show ip cache verbose flow

  This condition has been observed when the network topology is that for a typical Service Provider application where on an Cisco ASR 1000 Router that is configured as the PE and is sending packets to another router or host which is configured as the CE. The ASR PE-CE interface is configured for IPV4 only and has egress netflow configured on it. Packets entering the ASR 1000 Router must be MPLS encapsulated for this defect to be visible. If the packets entering the ASR 1000 Router are simple IPV4 packets the defect is not seen. Also the defect is not seen for packets taking the reverse path which is to say ingress netflow configured on the PE-CE interface where packets enter the box as IPV4 and leave as MPLS encapsulated packets.

  Workaround: There is no known workaround for Egress Netflow. Some information can be obtained by running ingress Netflow on the PE-CE interface. Also, as noted, if packets entering the box are IPV4 only, egress Netflow functions normally.

- CSCth96398

  Static Global MPLS routes may change labels after SSO causes traffic to drop on the ASR 1000 Router Series.

  This condition may occur when static global mpls routes change labels after SSO causes the traffic to drop on the router.

  Workaround: There is no workaround.

- CSCti09658

Some of the SRTP calls were hung after RTP with SRTP traffic exceeds the max support rate.

This conditions may occur when RTP with SRTP traffic exceeds the max support rate.

Workaround: There is no workaround.

- CSCti10518

  Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the rib.

  This condition has been observed when redistribution is occurring into EIGRP and the route ownership is changing in the middle of the redistribution process, EIGRP may leak the ndb in process.

  Workaround: There is no workaround.

- CSCti27989

  An ASR 1000 Router may show incorrect stats for exporter clients.

  This will happen when an exporter has multiple clients, for example an exporter being used by two flow monitors at the same time.

  Workaround: Use only one client per exporter.

- CSCti45918

  Show ip mroute vrf abc x.x.x.x count displays zero packets for an active m-cast stream.

  Ths condition has been observed when then DMVPN spoke tunnels are in a vrf instance and the tunnel source interface is iin global table.

  Workaround: Enable **ip pim sparse-mode** on tunnel-source interface in global table.

- CSCti48585

  Loss of connectivity on a SPA-4XCT3/DS0 when performing a manual ISSU subpackage upgrade on ESP's in an Cisco ASR 1000 Router. This condition has been observed upon performing a manual ISSU subpackage upgrade from version IOS XE 2.4.4 on the ESP's with SPA-4XCT3/DS0 configured this may cause the traffic to stop passing.

  Workaround: Perform the upgrade using a consolidated package method or by loading packages from packages.conf and reload.

- CSCti57128

  When CUBE(SP) is configured on the Cisco ASR 1000 Router, during an upgrade the configuration using header-profiles which reference privacy headers or privacy parameters fail to migrate correctly.

  An error is generated stating that cac-policy should be used to modify privacy settings. However no **cac-policy** commands exist to allow the re-configuration.

  For example:

```
sbc <name>
  sbe
    sip header-prrofile <name>
       header Privacy
       header-Remote-Party-ID
```

  Workaround: The solution allows seamless upgrade of these commands.

- CSCti59562

  DHCP accounting stop does not clear IP initiated session and radius-proxy sessions after CoA account logon / logoff / logon sequence. This condition has been observed when VRF mapping is being used on an Cisco ASR 1000 Router.

Workaround: There is no workaround.

- CSCti62355

  An unexpected reload may be seen on an ASR 1000 Series with Flexible Netflow configurations containing multiple flow monitors with exporters.

  This condition may occur on a router that has IP unicast and multicast configured, when multiple monitors are configured for flow monitoring by attaching them to one or more interfaces, issuing a **show ip cache flow** can result in an ESP reload.

  Workaround: There is no workaround.

- CSCti70690

  SBC causes ASR 1000 to reload, hitting CHECK failure (dumping diagnostics) and then an unhandled exception.

  The condition has been seen if CHECK and reload (exception) occurs when the following call flow takes place:

  – A call is made and successfully answered.

  – The callee chases the 200 INVITE response immediately with a BYE request. (These messages are so close together that they are processed by SBC in the same N-BASE schedule.)

  – SBC hits a CHECK failure while processing the BYE request, and passes on the 200 INVITE response.

  – The caller receives the 200 INVITE and sends an ACK.

  – SBC hits an unhandled exception while processing the ACK from the caller.

  This also requires that there is a subscriber registered through an ASR 1000 Router; or that a switchover has been performed, otherwise the failure is not seen when this flow occurs.

  Workaround: Do not use core with access type adjacencies.

- CSCti76872

  Interface names are truncated in the Flexible Netflow feature CLI output, such as in the following example:

```
Auto-MCP2#sh run int gigabitEthernet 0/2/6.6666666
Building configuration...
Current configuration : 129 bytes
!
interface GigabitEthernet0/2/6.6666666
 encapsulation dot1Q 6
 ip vrf forwarding vpn6
 ip address 115.0.6.1 255.255.255.0
end
Auto-MCP2#sh ip cache flow
SrcIf        SrcIPaddress   DstIf        DstIPaddress    Pr SrcP DstP  Pkts
Local         15.1.1.4       Tunnel4*      224.0.0.10     58 0000 0000  71
Tunnel3      113.0.3.2       gi0/2/6.3    115.0.3.2       ff 0000 0000  548  K
```

  This condition may be seen when Flexible Netflow on the ASR 1000 Router Series on "long" interface names.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.1.1S

All the caveats listed in this section are resolved in Cisco IOS XE Release 3.1.1S

- CSCtb58282

  Device running IOS may reload when **show tcp brief** is issued.

  This condition as observed when the following has occurred:

  1. The “ip domain lookup” command needs to be configured. It is on by default.
  2. The ip address of the foreign host in the tcp session needs to have a very long domain name associated with it, on the order of 70 characters.
  3. The port number of the foreign host needs to be 5 digits long.

  If **ip domain lookup** is **disabled**, the problem could still happen if the host has a static entry configured with the **ip host** command.

  Workaround: Configure **no ip domain lookup** or avoid using s**how tcp brief** on the device.

- CSCtf05408

  IP address on a loopback interface is lost.

  Workaround: Reconfigure the loopback interface.

- CSCtg11491

  System may encounter CPUHOG and an error message with the following traceback:

  ```
  %SYS-3-CPUHOG: Task is running for (2302)msecs, more than (2000)msecs (1/1), process =
  Exec
  ```

  After clearing 4k+ ISG RADIUS Proxy sessions through the CLI : clear radius-proxy client <ip address>.

  This symptom is observed on a Cisco ASR 1000 Router Series when functioning as an Intelligent Service Gateway (ISG) RADIUS Proxy after thousands of sessions are established.

  Workaround: There is no known workaround.

- CSCtg30995

  Delay of RP switchover associated with NV_BLOCK_INITFAIL message is appearing on standby turned- active RP console.

  This problem may occur when the manual switchover command, **redundancy force-switchover** and a filesystem command like **copy running-config startup-config** is issued from different Active RP consoles almost at the same time.

  Workaround: Avoid issuing any filesystem access command simultaneously with the manual RP switchover command. Should the above problem occurs, execute the same filesystem command, by issuing **copy running-config startup-config** from the standby-turned-active console.

- CSCtg52483

  SPA-1XCHOC12/DS0 reloads while BERT is running on the same results into malfunctioning of the router.

  This condition has been observed while BERT test is running, the SPA OIR resulted in BERT test hanging situation and afterwards the router does not allow for the BERT test to start anew. In addition, the previous BERT run is shown in running state even when **no bert** command is issued to stop the sequence.

  Workaround: There is no workaround.

- CSCth25661

  Plim qos scheduling commands disappear from running config on the standby RP if the SPAis stopped while the standby is down.

The following are the steps which may likely cause this problem:

1. Bring the standby RP down.
2. Configure an interface on the active RP.
3. Stop the SPA.
4. Bring the standby up.
5. Switchover to the standby RP and start the SPA.

Workaround: Stop the SPA when the standby is up and perform a switchover.

- CSCth50961

  POS configuration is not supported on the SPA-1XCHSTM1 SPA. However if you have the unsupported configuration on this SPA the router may fail repeatedly when booting the router.

  Workaround: Is to remove the unsupported POS configuration.

- CSCth59072

  After reloading ASR 1000 Router the backup interface is stuck to up instead of standby sometimes.

  This happens when using IOS XE 2.4.2 Release, or possibly later IOS XE releases.

  Workaround: Is to flap the affected interface.

- CSCth62425

  When trying to add a static and extendable NAT rule for port 80 or 443 (PAT), the operation fails with this error message:

  %Port 80 is being used by system min80

  or

  %Port 443 is being used by system min443

  This condition has been observed when upgrading from IOS Release 12.2(33)XND to 12.2(33)XNF and the following has occurred:

  - Add NAT rule for either port 80 or 443.
  - Delete NAT rule.
  - Add the same nat rule with a different Inside Local address.
  - Delete NAT rule.
  - Try to add the original NAT rule.
  - At this point, no other static nat rule can be added with the same Inside Global and port 80/443

  Workaround: Perform the following steps:

  1. Make sure that the HTTP port and secure-port are assigned to other than 80 and 443, respectively, and enable them.

  For example:

```
ip http port 10500
ip http secure-port 11000
ip http server
ip http secure-server
```

  2. Configure the port static mappings for the above ports for 80 and 443.

  For example:

```
ip nat inside source static tcp 10.50.50.50 80 10.1.1.4 80 extendable
ip nat inside source static tcp 10.50.50.50 443 10.1.1.4 443 extendable
```

3. Change these HTTP ports back to 80 and 443.

For example:

```
ip http port 80
ip http secure-port 443
```

4. Afterwards, the above port static mappings can be deleted and then added again, normally.

- CSCth64507

  Bulk Sync failure is seen on redundancy force-switcover command when eem policy is configured and policy file is present in only the Active RP.

  The failure is seen only when the policy file is present in a Active RP and not in a Standby RP.

  Workaround: Is to have the policy file present in both the Active RP and Standby RP.

- CSCth70149

  Wr mem fails after entering the command **verify nvram:startup-config** on a Cisco ASR 1000 Router.

  The following example identifies a Cisco ASR 1000 Router that is running Cisco IOS Software Release 12.2(33)XNE2:

  router#verify nvram:startup-config

  Verifying file integrity of nvram:startup-config...

  Embedded Hash SHA1 : 0A210A21204C61737420636F6E66696775726174

  Computed Hash SHA1 : 523416EF6B0CE417B3E12FFBA3491131B8821234

  Embedded hash verification failed for file nvram:startup-config.

  router#

  MEST: %SIGNATURE-3-NOT_VALID: %ERROR: Signature not valid for file nvram:startup-config.

  Router#wr

  startup-config file open failed (Device or resource busy)

  This condition has been seen when the ASR 1000 is running 12.2(33)XNE2.

  Workaround: Is to reload the router.

- CSCth70566

  %ASR1000_RP_SPA-3-VC_FLOWID_ALLOC_FAIL messages are shown on the console after RP switchover.

  The issue may happen if additional ATM PVCs are configured and an RP switchover has happened.

  Workaround: There is no workaround.

- CSCth72829

  When trying to enable Virtual Fragmentation Reassembly feature the same in the interface level configuration is unable to be seen.

  As shown in the following configuration example:

  ASR(config)#int gig 2/0/0

ASR(config-if)#ip v?

verify vrf

This condition may occur when the ASR 1000 is running IOS XE using IPBASE feature sets.

Workaround: None

- CSCth96093

  When the Cisco ASR 1000 platform is configured with Fast Re-Route for Traffic Engineering purposes the router will lose their backup tunnel after performing ISSU procedure. The primary tunnel will continue to function and there is no permanent traffic loss. However, if the primary tunnel fails for any reason, there will be no backup tunnel to fall back on.

  The problem may happen when ISSU downgrade from an IOS XE version 3.1.1S or higher to version 3.1.0 is done, after a redundancy forced switchover in the ISSU procedure.

  Workaround: The problem can be addressed by re-applying the traffic engineering backup-path command on the interface after the ISSU downgrade and after the box has been forced onto the newly downgraded route processor.

  For example:

  MCP-6RU-2(config-if) # mpls traffic-eng backup-path <Tunnel #>

- CSCti01831

  Standby ESP may get stuck in init state.

  This condition has been observed after performing an ISSU downgrade to a IOS XE 3.1S image.

  Workaround: There is no workaround.

- CSCti05253

  When POS interface has been created using SPA-1XCHOC12/DS0 the SPA is no longer accessible, after performing an OIR for the slot in which the SPA is present.

  This instance may always occur whenever an OIR has performed in the slot in which the SPA-1XCHOC12/DS0 is present.

  Workaround: There is no known workaround.

- CSCti05925

  The DTMF interworking function of IPIP gateway is not working, properly. The DTMF relay of one format converts to another DTMF relay format by IPIP gateway

  The problem may exist on the ASR 1000 platform or other platforms when running BINOS.

  Workaround: There is no workaround.

- CSCti06235

  Firewall cannot send out HSL packets on ESP40. The destination IP is reversed in the datapath.

  This condition may occur after configuring Firewall HSL on ESP40.

  Workaround: Configure a reversed destination IP.

- CSCti10146

  On injecting LAIS into POS interface, PRDI is seen together with LAIS.

  This issue has been seen on an Cisco ASR 1000 Router running IOS XE Release versions, staring from 2.5.0 and onwards.

  Workaround: There is no workaround.

- CSCti41837

  Clear Channel POS interface configured on Channelized OC12 card might stay up/down in case of Path

  alarms.

  This condition has been observed when the following steps have been executed:

  1. Insert Path alarm such as PAIS with path delay triggers enabled
  2. Insert Line alarm such as SLOS
  3. Remove Line alarm

  The above steps would result in POS interface being stay up/down in case Path alarm PAIS present.

  Workaround: Controller **sh/no sh** would bring POS interface back to down/down state.

- CSCti58920

  The following error message is observed when SPA-4XT-SERIAL is housed in ASR1000-SIP40:

  %SPA_OIR-3-UNSUPPORTED: The SPA-4XT-SERIAL (0x55A) in subslot 0/0 is not supported by the ASR1000-SIP40 module

  The symptom is observed when SPA-4xT-Serial SPA is configured on the ASR1000-SIP40 running Cisco IOS XE 3.1.0S Release.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.1.0S

This section documents possible unexpected behavior by Cisco IOS XE Release 3.1.0S

- CSCsz79432

  While sending traffic from the RTR1 to RTR2 outgoing interface network, RTR2 is not forwarding directed broadcast when enabling ip directed-broadcast on an ASR 1000 Router.

  This condition has been observed when enabling ip directed-broadcast on the router, while sending traffic from the RTR1 to RTR2 outgoing interface network, RTR2 is not forwarding directed broadcast

  Workaround: There is no workaround.

- CSCsz82080

  Under a scaled configuration (e.g. 1500 DVTI remote access sessions), when bringing up all the 1500 sessions at the same time in the DVTI server, the ESP may also reload.

  This condition has been observed when bringing up 1500 DTVI sessions simultaneously.

  Workaround: Is to bring up 100 Virtual Access interfaces at one time.

- CSCtg18977
  RP reloads when it detects that the control plane has locked up.

  This condition occurs with a high amount of punted traffic specifically when the system is running with LARGE amount of BGP sessions.

  Workaround: There is no workaround.

- CSCtg60941
  When attempting to establish a BGP adjacency from an interface in an IPv4 VRF address family to a peer accessible through the global routing table fails.

This is occurs when one neighbor IP address is in a VRF address family and the other neighbor address is accessible via the global routing table using static routes to leak the routes between the two routing tables.

Workaround: There is no workaround.

- CSCtg78972

  Memory Leak in FMAN-ESP ACL.

  The memory allocated by “acl” module in FMAN-ESP keeps growing by ~128 bytes for each ~28K PPPoEoA flapping.

  This condition may occur when there are flapping PPPoEoA sessions.

  Workaround: There is no workaround.

- CSCtg88383

  ESP40 occasionally gets stuck in “init, active” state during reboot.

  This problem is seen during ESP reboot.

  Workaround: No workaround is required. After about 300 seconds, RP reboots ESP40 and ESP40 comes up fine next time.

- CSCtg90378

  An Cisco ASR 1000 Router may take ~18 - 20+ minutes to boot completely and during the course the IOS CUP remains high at 99.9%.

  This condition may be seen with high FW and NAT scaled configurations.

  Workaround: There is no workaround.

- CSCtg95994

  MLP bundle interface fails to come up properly with the following error message:

  QFP:00 Thread:126 TS:00000002037602773659 %QFP_MLP-3-PROXY_DUP_LINK_ID:

  QFP MLP Proxy (Rx LINK-ADD) duplicate Link ID ...

  and will not forward traffic.

  This can occur if a MLP bundle with multiple member links is torn down and recreated several times.

  Workaround: There is no workaround.

- CSCth08631

  When the outbound traffic is fragmented packets, the second and on-going fragments do not contain any L4 information about the ASR 1000 Router. However, there maybe some false positive matches on an output ACL.

  This condition are observed when outbound traffic is fragmented packets and some false positive matches on an output ACL has occurred.

  Workaround: Create very specific ACLs using specific IPs for all entries that are not scalable.

- CSCth11310

  IP-subscriber sessions stop forwarding traffic after RADIUS proxy resets them. The session does not appear to get any traffic, and drops may be observed when the following command is used:

  show platform hardware qfp active statistics drop

  This behavior may occur on ASR 1000 Router Series, with routed IP-subscriber sessions that are reset and converted to RADIUS proxy sessions.

Workaround: There is no workaround.

- CSCth24984

  High CPU usage on when RP1 is configured as the DMVPN hub. This condition may occur when having 1000 Static BGP neighbors (spokes) over the DMVPN hub.

  Workaround: There is no workaround.

- CSCth27728

  After SBC has been configured on an ASR 1000 Router, and a SIP call is made. The router reloads.

  This condition has been seen when the **del-prefix 0** instructs SBC to remove the first zero digits from a dialed number, which means not doing anything. SBC does not handle being instructed to remove zero digits from the number and this is may cause a failure. Removing this from the config should result in the same behavior and may avoid the router to fail.

  Workaround: By removing **edit del-prefix 0 add-prefix 64** rom the config and replacing it with **edit del-prefix 1 add-prefix 64** this should prevent the router from failing.

- CSCth36539

  IPv6 Video on demand traffic is not forwarded by ESP 40.

  This condition can occur when the number of VoDv6 are scaled (> 300 sbc pinholes), traffic for IPv6 VoD destinations will not be forwarded by ESP 40.

  Workaround: Is to reduce the number of VoDv6 pinholes to 1.

- CSCth37116

  IP Accounting feature is not supported on the Cisco ASR 1000 Router Series. This only applies to the Cisco ASR 1000 Router Series.

  Workaround: Do not configure IP Accounting on Cisco ASR 1000 Router Series.

- CSCth41121

  An ASR 1000 Router may reload while processing a renegotiation rejection (reINVITE 491) on a call which is being transcoded. This condition occurs when a reINVITE is rejected (a renegotiation failure) on a call which is already established and not using a transcoder. The reINVITE was attempting to use a transcoder (the new stream needed transcoding). The trigger for this failure is that the renegotiation adds an extra stream to the call (a new m= line in the SDP) and the reINVITE is rejected.

  Workaround: There is no workaround.

- CSCth41321

  Standby ESP reloads after repeated RP switchovers. This conditions has been seen when PPPoX sessions with ISG features in a dual RP with dual ESP configuration. After many repeated switchovers have occurred while sessions continue to be setup, the standby ESP may fail.

  Workaround: No known workaround.

- CSCth43945

  QFP might reload when scaled configuration of GRE with QoS is loaded, and the physical interface state is up/down quickly.

  This condition has been observed when the ASR 1000 is configured with a large number of GRE tunnels with QoS service-policy, and the physical port used by the GRE tunnels have experienced the link state up/down within a short interval, the QFP might be reloaded due to one critical process getting reset.

  Workaround: There is no workaround.

- CSCth45487

  On a Cisco ASR 1000 Router a cpp_cp_svr reload has been observed while booting up with NAT configurations.

  This problem may occur on the router when there are high amounts of traffic sent, and low memory condition occurs.

  Workaround: There is no workaround.

- CSCth48147

  SBC hits a CHECK failure (and dumps diagnostics files) when processing a BYE rejection response.

  This CHECK failure occurs (on SBC version 2500_065) when the following call scenario takes place:

  – A call is set up between caller and callee. SIP to SIP call. Delta renegotiation is configured (the default behavior).

  – A reINVITE, which changes the media (for example, a codec change) is sent from the caller and received at the callee. No response is yet sent.

  – A BYE is sent from the caller to the callee. No response is yet sent.

  – The callee then responds to the reINVITE with a 481 error code. This causes SBC to start to tear down the call.

  – Immediately after sending the 481 reINVITE response, the callee sends a 491 BYE response (the same reload occurs if this is some other error codes, but it must not be 481 or 200). When SBC processes the 481 reINVITE response and 491 BYE response in quick succession, the Check failure occurs.

  Workaround: None

- CSCth48281

  SBC reloads when processing a 302 INVITE response. This is due to a problem on a forked call previously.

  Reload occurs after a forked call in which SBC processes two incoming calls with the same Call-ID and From tag. One of these calls is answered and before either an answer on the other call or an ACK on the first call, the callee sends a BYE to SBC. SBC fails due to being unable to correctly correlate the BYE with the right call.

  Workaround: There is no workaround.

- CSCth48869

  Console Freeze (Lock) and iosd CPU remains at 99.9% for more than 45 minutes. This happens when unconfiguring and reconfiguring QoS on the interfaces which are configured for NAT / FW redundancy. This happens when 75 - 200 interfaces are unconfigured and configured for QoS.

  Workaround: There is no workaround.

- CSCth50961

  POS configuration is not supported on the SPA-1XCHSTM1 SPA. However if you have the unsupported configuration on this SPA, the router reloads repeatedly when the router is booted.

  Workaround: Remove the unsupported POS configuration.

- CSCth53652

  SBC reloads while processing a BYE response from an endpoint before a call has been connected when the caller has sent a BYE followed by a CANCEL.

This occurs when the following call flow is seen:

1. INVITE from caller to callee.
2. Callee sends provisional response back (for example, 180).
3. Caller sends BYE to callee.
4. Caller then sends CANCEL to callee.

   This will cause SBC to return 487 INVITE response (and 200 CANCEL) and start call teardown. SBC will also respond 481 to the BYE from the caller, and forward the CANCEL to the callee.
5. Callee then sends 200 BYE response, which causes the problem.

Workaround: There is no workaround.

- CSCth59072

  After reloading ASR 1000 Router the backup interface is stuck to up instead of standby sometimes.

  This happens when using IOS XE 2.4.2 Release, or possibly later IOS XE releases.

  Workaround: Is to flap the affected interface.

- CSCth60620

  XE31 Kernel core needs to be processed off-router due to utility changes. If a Cisco ASR 1000 Series Router experiences a kernel core, it will require off-loading for processing. Kernel cores are large when compressed (at about 2GB or more) and will expand to 8GB to up to 16GB depending on the RP memory capacity. The utility, crash, used to examine these cores dynamically links to other libraries, so it cannot be run on an ASR 1000 with the same image. There are concerns about storage on the router being sufficient if one could be decoded on an ASR 1000 (easily worked around). Having the correct vmlinux and map file is required.

  Workaround: Use the recommended procedure. Make sure that the target file system supports files of up to 16GB and is running the proper version of Linux.

- CSCth62425

  When trying to add a static and extendable NAT rule for port 80 or 443 (PAT), the operation fails with this error message:

  ```
  %Port 80 is being used by system min80
  or
  %Port 443 is being used by system min443
  ```

  Workaround: There is no workaround.

- CSCth66196

  Static NAT with “no-payload” option breaks if zone-based firewall is enabled on the ASR 1000 Router Series.

  Without Zone-based Firewall configured on the router, NAT works.

  Workaround: There is no workaround.

- CSCth67494

  Some packets from captive portal to client are not hitting the redirect translations.

  The precise conditions are not known but this seems to be related to activating/deactivating new services on subscriber session.

  Workaround: There is no workaround.

- CSCth68125

SNMP MIBS counter for output/input packets/bytes such as ifOutOctets, ifHCOutOctets, ifHCOutUcastPkts and similar counters will not increment on multiple subinterface. After issuing **show vlan** counter command this will not allow for the increments to increase on an interface.

Note When a large number of subinterfaces are presented under the main interface, the stat update will take a longer time. This may take up to few secs or minutes based on number of subinterface configured with traffic in Release 2.5.0.

This condition may persist when there are multiple subinterfaces configured and the main interface went into tunnel/L2-transport mode. The above condition has been seen on ASR 1000 Router Series.

Workaround: There is no workaround for Release 2.5.0.

For Release 2.6.0 and later releases: Configure ***hw-module subslot <> ethernet vlan unlimited***

Recovery: Is to perform **shut/no shut** on the main interface, if this condition still persist then reload the SPA.

Note The above workaround and recovery mechanism will impact traffic.

- CSCth70149

  Wr mem fails after entering the command **verify nvram:startup-config** on a Cisco ASR 1000 Router.

  The following example identifies a Cisco ASR 1000 Router that is running Cisco IOS Software Release 12.2(33)XNE2:

  router#verify nvram:startup-config

  Verifying file integrity of nvram:startup-config...

  Embedded Hash SHA1 : 0A210A21204C61737420636F6E66696775726174

  Computed Hash SHA1 : 523416EF6B0CE417B3E12FFBA3491131B8821234

  Embedded hash verification failed for file nvram:startup-config.

  router#

  MEST: %SIGNATURE-3-NOT_VALID: %ERROR: Signature not valid for file nvram:startup-config.

  Router#wr

  startup-config file open failed (Device or resource busy)

  This condition has been seen when the ASR 1000 is running 12.2(33)XNE2.

  Workaround: Is to reload the router.

- CSCth71105

  ESP20 core after “no SBC” under high rate traffic (CPS=58/HT=180) for RTP with SRTP traffic for an hour.

  This condition has been observed when RTP with SRTP traffic ESP20 after "no SBC" under high rate traffic has occurred.

  Workaround: There is no workaround.

- CSCth72507

  When an ASR 1000 Router has attached running config the active secondary keeps reloading.

Workaround: There is no workaround.

- CSCth72829

  When trying to enable Virtual Fragmentation Reassembly feature the same in the interface level configuration is unable to be seen.

  As shown in the following configuration example:

  ASR(config)#int gig 2/0/0

  ASR(config-if)#ip v?

  verify vrf

  This condition may occur when the ASR 1000 is running IOS XE using IPBASE feature sets.

  Workaround: None

- CSCth72869

  Changes in adjacencies during RP switchover while running WCCP may trigger IOS reload with the following message:

  ```
  ASR1000-EXT-SIGNAL: U_SIGABRT(6), Process = Net Background
  ```

  The following error may be seen shortly before the reload:

  ```
  %FMANRP_OBJID-5-DUPCREATE: Duplicate forwarding object creation obj_handle <hex
  value>, type <number>, existing obj_id <hex value>, type <number>
  ```

  Workaround: Disable WCCP.

- CSCth72971

  Unexpected ESP reload may occur, accompanied by the following error message:

  %OOM-3-NO_MEMORY_AVAIL: F1: oom.sh: The system is very low on available

  memory. Operations will begin to fail.

  The router's configuration includes multiple **deny** statements.

  Workaround: Remove the deny statements from the config.

- CSCth73260

  QFP reload my occur or output indicates 0 translation when there are translations. In addition, a traceback may also occur.

  This occurs upon entering **sh ip nat trans** with more then 250 static networks or upon entering **sh ip nat trans verb** with more then 50 static networks.

  Workaround: Reduce the number of static networks or avoid these commands. This problem is expected to be correct in IOS XE 3.1.1S Rebuild.

- CSCth75324

  Throughput degradation is about 8% compared to Release 2.6.0 when MPLS SETVRF feature is configured on the ASR 1000 Router Series.

  In Release 2.6.0, throughput was 12.31 Mpps with RP1/ESP10. However, in Release 3.1.0S, throughput is 11.29 Mpps with RP1/ESP10.

  This condition has been observed when an ASR 1000 is configured with PBR set VRF+L3VPN with 500 VRFs this will cause the throughput performance degradation.

  Workaround: There is no workaround to increase the performance.

- CSCth76964

The following command: **sh platform hardware slot <slot-num> plim qos input bandwidth** command doesn't display the configured values for policer and weight configuration on CC40.

The problem is seen on CC40 only when it has an ATM SPA. The configured values are not displayed for the other SPAs sitting next to ATM SPA in the same bay but doesn't have any functionality impact.

Workaround: Perform **hw-module subslot <slot/subslot> shut** on the ATM SPA and the configured values can be seen in the **show** command output.

- 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