Caveats in Cisco IOS XE 3.3S Releases

This chapter provides information about caveats in Cisco IOS XE 3.3S 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 3.3S 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 3.3S 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 contains the following topics:

Open Caveats—Cisco IOS XE Release 3.3.2S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.3.2S.

- CSCtr16465

  Symptoms: During Cisco IOS XE Release 3.2 to Cisco IOS XE Release 3.4 and Cisco IOS XE Release 3.3 to Cisco XE Release 3.4 ISSU upgrade or downgrade tests with MPLS features on both 4RU and 6RU, pending-issue is seen.

  Conditions: This symptom occurs only MPLS features.

  Workaround: There is no workaround.

- CSCtr16637

  Symptoms: Active RP2 crashes.

  Conditions: This symptom may occur while activating or deactivating billing over and over under 200 CPS NNI call and both XML and radius billing are enabled. This may result in check failure getting printed.

  Workaround: There is no workaround.

- CSCtr31773

  Symptoms: RP crashes.

  Conditions: This symptom occurs with the following conditions:

  1. Header manipulate feature is enabled, and changes have been made.
  2. Swtichover takes place.

  Workaround: There is no workaround.

- CSCtr38720

  Symptoms: Outbound calls fail due to code 47 error on Cisco ASR CUBE-ENT.

  Conditions: Outbound calls fail on the Cisco ASR router due to an issue with the communication between the control and data plane of the Cisco ASR router.

  Workaround: Reload the router.

- CSCtr39816

  Symptoms: SBC crashes due to assert failure.

  Conditions: SBC crashes when using Header Manipulation feature to do IP-FQDN for OPTION ping message. But when making a basic SIP call, the assert occurs and SBC crashes.

Workaround: There is no workaround.

- CSCtr47472

  Symptoms: Routes do not get added again after removing redistribute route-map.

  Conditions: This symptom occurs while using the following commands:

  – **Redistribute ospf 1 match internal ext 1 ext 2 route-map empty_map**

  – **No Redistribute ospf 1 match internal ext 1 ext 2 route-map map1**

  Workaround: There is no Workaround.

- CSCtr56484

  Symptoms: Username attribute received in access-accept is not used by ISG as session-handle.

  Conditions: This symptom occurs when the username received by an ISG client needs to be over-written by contents of username (attribute1) response from Radius.

  Workaround: There is no workaround.

- CSCtr56576

  Symptoms: Cisco ASR router QFP crashes indicating either fragmentation or reassembly of packets.

  Conditions: This symptom occurs with QOS(service-policy) while using **set mpls experimental imposition** command in policy-map configuration.

  Workaround 1: Remove service-policy applied to the interface.

  Workaround 2: Downgrade to Cisco IOS Release 15.1(1)S2.

- CSCtr65254

  Symptoms: System core runs after 24, 48, and 72 hour traffic.

  Conditions: This symptom may occur after 24, 48, and 72 hour traffic.

  Workaround: There is no workaround.

- CSCtr74460

  Symptoms: Shutting down the GigabitEthernet0 interface on Cisco ASR1000 series routers with RP2 Route Processor card does not bring the link down. The LED of GigabitEthernet0 interface and the connected port on the switch are all in green.

  Conditions: This symptom occurs when a Cisco ASR1000 series router with RP2 Route Processor card is connected to a switch using GigabitEthernet0 interface.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.3.2S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.3.2S.

- CSCti98219

  Symptoms: The router crashes upon transmission of MPLS-labeled packet.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(24)T3 or Cisco IOS Release 15.0(1)M3. However, others may be affected. The router acts as an MPLS/VPN PE with VRF-NAT. This issue is seen when SIP packets are sent on the MPLS-facing interface.

  Workaround 1: Filter SIP traffic inbound on the IP-facing interface.

  Workaround 2: Configure “no ip nat service sip udp port 5060”.

- CSCtj14525

  Symptoms: Standby is not synced to active after attaching a new policy.

  Conditions: This symptom occurs when a dynamic policy is used such as RADIUS CoA.

  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.

- CSCtk67768

  Symptoms: RP crash is observed in the DHCPD receive process.

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

  Workaround: There is no workaround.

- CSCtk69114

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

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

  Workaround: There is no workaround.

- CSCtl00995

  Symptoms: Cisco ASR 1000 series routers with 1000 or more DVTIs may reboot when a shut/no shut operation is performed on the tunnel interfaces or the tunnel source interfaces.

  Conditions: This symptom occurs when all the DVTIs have a single physical interface as the tunnel source.

  Workaround: Use a different tunnel source for each of the DVTIs. You can configure multiple loopback interfaces and use them as the tunnel source.

- CSCtn18784

  Symptoms: Interface Tunnel 0 constantly sends high bandwidth alarms.

  Conditions: The conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtn19027

  Symptoms: The **show mediatrace responder sessions brief** command crashes the router.

  Conditions: This symptom is observed on Mediatrace Responder when showing a stale session.

  Workaround: There is no workaround. Avoid issuing this impacted **show** command.

- CSCtn44232

  Symptoms: With multiple RP switchovers, both RPs become unusable.

  Conditions: This symptom is observed with multiple RP switchovers.

  Workaround: There is no workaround.

- CSCtn58128

  Symptoms: BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.

  Conditions: This symptom may be triggered by route-flaps in a scaled scenario, where the route reflector may have 4000 route reflector clients and processing one million+ routes.

  Workaround: Ensure “no logging console” is configured.

- CSCtn68117

  Symptoms: Session command does not work on Cisco C3K series routers that have become the master after a mastership change.

  Conditions: This symptom is seen when failover to slave occurs.

  Workaround: There is no workaround.

- CSCtn96521

  Symptoms: When the Spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors fail to establish adjacency.

  Conditions: This symptom is observed when the Spoke (dynamic) peer group is configured before the iBGP (static) peer group.

  Workaround: If the order of creation is flipped, the two iBGP (static) neighbors will establish adjacency.

- CSCtn97451

  Symptoms: The bgp peer router crashes after executing the **clear bgp ipv4 unicast** *peer* command on the router.

  Conditions: This symptom occurs with the following conditions:

  ```
  Router3 ---ebgp--- Router1 ---ibgp--- Router2
  ```

  ROUTER1:

  ```
  interface Ethernet0/0
      ip address 10.1.1.1 255.255.255.0
      ip pim sparse-mode
  !

  router ospf 100
      network 0.0.0.0 255.255.255.255 area 0
  !

  router bgp 1
      bgp log-neighbor-changes
      network 0.0.0.0
      neighbor 10.1.1.2 remote-as 1
      neighbor 10.1.1.3 remote-as 11 !
  ```

  ROUTER2:

```
interface Ethernet0/0
   ip address 10.1.1.2 255.255.255.0
   ip pim sparse-mode
!
router ospf 100
   redistribute static
   network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
   bgp log-neighbor-changes
   network 0.0.0.0
   redistribute static
   neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

ROUTER3:

```
interface Ethernet0/0
   ip address 10.1.1.3 255.255.255.0
   ip pim sparse-mode
!

router bgp 11
   bgp log-neighbor-changes
   network 0.0.0.0
   network 0.0.0.0 mask 255.255.255.0
   redistribute static
   neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

Crash reproduce steps are as follows:

1. Traffic travel from ROUTER3 to ROUTER2.
2. "clear bgp ipv4 unicast 10.1.1.1" on ROUTER2.

Workaround: There is no workaround.

- CSCto00796

  Symptoms: In a rare and still unreproducible case, the RR (also PE) misses sending the RT extended community for one of the redistributed VPNv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR).

  Conditions: This symptom occurs when a new interface is provisioned inside a VRF and the configuration such that the connected routes are redistributed in the VRF. This redistributed route fails to tag itself with the RT when it reaches the peering PE (+RR)

  Workaround: Soft clear the peer that missed getting the RT.

- CSCto07586

  Symptoms: An IPV4 static BFD session does not get established on a system which does not have IPV6 enabled.

  Conditions: This symptom occurs with the following conditions:

  1. Create an IOS image that does not have IPV6 enabled.
  2. Enable BFD on an interface.
  3. Configure an IPV4 static route with BFD routing through the above interface.

The IPV4 BFD session does not get established, so the static route does not get installed.

Workaround: Unconfigure BFD on the interface, and then reconfigure it. Then, the session will come up.

- 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.

- CSCto16106

  Symptoms: Address is not assigned when “ip dhcp use class aaa” is configured.

  Conditions: When the DHCP server is configured to download a class name from the radius using “ip dhcp use class aaa” and lease an IP address from that class, the IP address is not assigned to the client.

  Workaround: There is no workaround.

- CSCto31265

  Symptoms: ABR does not translate Type7 when primary Type7 is deleted even if another Type7 LSA is available.

  Conditions: This symptom occurs with OSPFv3. ABR receives multiple Type7 LSA for the same prefix from Multiple ASBR.

  Workaround 1: Delete/readd the static route that generates Type7.

  Workaround 2: Execute the **clear ipv6 ospf force-spf** command on ABR.

  Workaround 3: Execute the **clear ipv6 ospf redistribution** command on ASBR.

- CSCto35160

  Symptoms: After switchover, traffic drops are seen in CARRIER-Ethernet testcase for about 15 seconds. This issue is not seen consistently.

  Conditions: This symptom is seen after switchover.

  Workaround: It will auto restore after 15 seconds.

- CSCto41165

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

  Conditions: This symptom occurs when the standby router is configured.

  Workaround: There is no workaround.

- CSCto41223

  Symptoms: The standby IOSD crashes when standby RP reload is executed.

Conditions: This symptom is observed in a scaled configuration with 8000 EoMPLS and 8000 EVC sessions while the traffic is flowing. On issuing standby RP reload, IOSD crashes at the process "Standby service handler".

Workaround: There is no workaround.

- CSCto46716

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

  Conditions: This symptom occurs when the MPLS TE tunnel is configured with forwarding adjacency. In "debug ip ospf spf", when 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 that not all tunnels are affected. It is unpredictable which tunnel is affected, but the number of affected tunnels grows with the number of configured tunnels.

  Workaround: If feasible, use autoroute announce instead of forwarding adjacency. Otherwise, upgrade to the fixed version.

- CSCto55643

  Symptoms: High CPU loading conditions can result in delayed download of multicast routes to line cards, resulting in multicast forwarding (MFIB) state on line cards out of sync with the RP. The **show mfib linecard** command shows line cards in sync fail state with many in LOADED state.

  Conditions: This symptom occurs during high CPU loading due to router reload or line card OIR events in a highly scaled multicast environment with high line rates of multicast traffic and unrestricted processed switched packets, before HW forwarding can be programmed.

  Workaround: There is no workaround. Ensure that mls rate limits are properly configured.

  Further Problem Description: IPC errors may be reported in the MRIB Proxy communications channel that downloads multicast routes to line cards.

- CSCto55983

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

  Conditions: This symptom occurs during high CPU utilization caused by multicast traffic. The **show mfib line summary** command does not show cards in sync.

  Workaround: There is no workaround.

- CSCto69071

  Symptoms: Metrics collection fails due to invalid DVMC runtime object handle.

  Conditions: This symptom occurs when the transport layer is not passing up an interface type that is acceptable to DVMC.

  Workaround: There is no workaround.

- CSCto72480

  Symptoms: The output of the **show mfib linecard** command shows that line cards are in "sync fail" state.

  Conditions: This symptom occurs usually when the last reload context displayed in the **show mfib linecard internal** command output is "epoch change". This indicates that an IPC timeout error has occurred in the MRIB communications channel that downloads multicast routing entries to the multicast forwarding information base (MFIB). In this condition, multicast routing changes are not communicated to the failed line cards and they are not in sync with the RP.

Workaround: If this issue is seen, using the **clear mfib linecard** *slot* command may clear the problem. If the problem occurs on a Cisco 7600 SP, an RP switchover is required after clearing the problem on any affected line cards. The workaround may not completely work if high CPU loading continues to be present and IPC errors are reported.

Further Problem Description: The IPC timeout errors could result from high CPU loading conditions caused by high rates of processed switched packets. High rates of multicast processed switched packets can be avoided if rate limits are applied after each router boot, especially after using the **mls rate-limit multicast ipv4 fib-miss** command.

- CSCto76018

  Symptoms: The Cisco ASR1000-WATCHDOG process crashes on DVTI Server after clearing crypto session on DVTI Client.

  Conditions: This symptom occurs for sessions with the configuration of 1000 VRFs, 1 IKE session per VRF, and 4 IPSec SA dual per session. The Cisco ASR1000-WATCHDOG process crashes on the DVTI Server during clear crypto session on the DVTI client, after all the SAs have been established.

  Workaround: There is no workaround.

- CSCto88581

  Symptoms: The standby RP crashes following an interface configuration change.

  Conditions: This symptom is observed only when “ospf non-stop routing” is configured.

  Workaround: There is no workaround.

- CSCto90252

  Symptoms: A standby route processor (RP) is stuck to “init, standby” for about 10 hours.

  Conditions: This symptom occurs after reloading five or six times on a Cisco ASR 1000 series router.

  Workaround: Disable NSR.

- CSCto98212

  Symptoms: The IPv6 address and prefix 2001:DB8:1:104::/64 at 25 Aug 2011 00:01 25 Jul 2011 00:01 are lost after a router realod.

  Conditions: This symptom occurs when this command checks for the clock validity. When the router reloads the clock validity is displayed as “not yet valid”. This causes the command to not be applied.

  Workaround: There is no workaround.

- CSCto99523

  Symptoms: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR).

  Conditions: This symptom occurs when convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR). There is no functionality impact.

  Workaround: There is no workaround.

- CSCtq04117

  Symptoms: DUT and RTRA have a IBGP-VPNv4 connection that is established via loopback. OSPF provides reachability to a BGP next hop, and BFD is running.

  Conditions: This symptom occurs under the following conditions:

  1. DUT has learned VPNv4 route from RTRA, and the same RD import is done at DUT.

2. When switchover is performed in RTRA and when GR processing is done, the route is never imported to VRF.

Workaround: Use the **clear ip route vrf x *** command.

- CSCtq06538

  Symptoms: The RP crashes due to bad chunk in MallocLite.

  Conditions: This symptom occurs while executing testcase number 4883. The test case 4883 sends an incorrect BGP update to the router to test whether the router is able to handle the problematic update. The incorrect BGP update has the local preference attribute length incorrect:

```
LOCAL_PREF
  Header
   AttributeFlags
    Optional: 0b0
    Transitive: 0b1
    Partial: 0b0
    ExtendedLength: 0b0
    Unused: 0b0 0b0 0b0 0b0
  TypeCode: 0x05
  Length: 0x01      <----- should be 0x04 instead
 Value: 0xff 0xff 0xff 0xff
NetworkLayerReachabilityInfo: 0x08 0x0a <snip>
```

  Workaround: There is no workaround.

- CSCtq22873

  Symptoms: The router may show the following traceback (error message) after receiving certain IPv6 packets:

```
TB:%SCHED-2-EDISMSCRIT:process=PuntInject Keepalive Process
```

  Conditions: This symptom when the router is configured for IPv6 routing.

  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

- CSCtq23793

  Symptoms: After reloading the PE router in the mVPN network, multicast traffic stops on one of the VRFs randomly.

  Conditions: This symptom occurs under the following conditions:

  - When reloading a PE in mVPN network.
  - When PE has many VRFs and scaled mVPN configuration.

  Workaround: Remove and add the MDT configuration.

- CSCtq32896

  Symptoms: LSM entries stop forwarding traffic.

  Conditions: This symptom is observed after Stateful Switchover (SSO).

  Workaround: There is no workaround.

- CSCtq43480

  Symptoms: A Cisco router crashes.

  Conditions: This symptom occurs when a session starts with PBHK and accounting features while the method list is not provisioned for the accounting features.

  Workaround: There is no workaround.

- CSCtq46745

  Symptoms: Custom configured default sip profiles (option/method/header) are lost during a router reload.

  Conditions: This symptom occurs during reload.

  Workaround: Use non-default profiles for each adjacency.

- CSCtq46760

  Symptoms: When doing ISSU subpackage upgrade from Cisco IOS XE Release 3.2.2 to Cisco IOS XE Release 3.4.0 with the Cisco IOS XE Release 2.3 feature set, both FPs crash and multiple core files are seen after the last ISSU step, active RP loadversion.

  Conditions: This symptom only occurs on Cisco ASR1006 subpackage upgrade with dual RPs.

  Workaround: Reload the standby RP before switchover.

- CSCtq56078

  Symptoms: Performance downgrade occurs after 8k SDP support.

  Conditions: This symptom occurs after SBC rejects the call if SDP is over 5k.

  Workaround: There is no workaround.

- CSCtq62759

  Symptoms: The CLNS routing table is not updated when the LAN interface with the CLNS router ISIS configured shuts down because ISIS LSP is not regenerated. The CLNS route will be cleared after 10 minutes when ISIS ages out the stale routes.

  Conditions: This symptom is seen when only the CLNS router ISIS is enabled on the LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

  Workaround: Use the **clear clns route** command or the **clear isis *** command.

- CSCtq83629

  Symptoms: The error message is associated with a loss in multicast forwarding state on line cards under scaled conditions when an IPC error has occurred.

  Conditions: This symptom is observed during router boot or high CPU loading, which can cause IPC timeout errors. This issue is seen on line cards during recovery from an IPC error in the MRIB channel.

  Workaround: Line card reload is required to resolve the problem.

- CSCtq92182

  Symptoms: An eBGP session is not established.

  Conditions: This issue is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.

  Workaround: Use an IPv6 neighbor address with bits. Set some higher bits, along with the IPv4 mapped address.

- CSCtq96329

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

  Conditions: This symptom can happen only when bgp deterministic-med is configured.

  The following releases are impacted:

  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp*** command or hardreset of BGP session to remove any stale prefixes.

- CSCtr07704

  Symptoms: While using scripts to delete nonexistent classmap filter from a class, the router sometimes crashes (c2600XM) or returns traceback spurious memory access (c2801nm).

  Conditions: This symptom occurs when trying to delete a nonexistent classmap filter, the classmap will be NULL, and passed to match_class_params_same. This results in referencing a null pointer.

  Workaround: Do null check in match_class_command and match_class_params_same. To keep the existing behavior, do not print out a message like “the class does not exist” when deleting a nonexistent class map from a class.

- CSCtr30820

  Symptoms: The IP address is not assigned to the client after a DHCP request.

  Conditions: The problem is observed while verifying the VRF-aware-DHCP functionality in Cisco IOS relay and server in an MPLS setup.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.3.1S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.3.1S.

- CSCtq46745

  Symptom: Default SIP profiles (option, method, or header) that were custom configured earlier are lost during a router reload.

  Conditions: This issue is observed when a router is reloaded.

  Workaround: Use nondefault profiles for each adjacency.

- CSCtq36726

  Symptom: Configuring **ip nat inside** command on the IPSEC dVTI VTEMP interface does not have any effect on the cloned virtual-access interface. The NAT functionality is thus broken, because the virtual-access interfaces does not get this command cloned from the respective VTEMP.

  Conditions: This issue occurs on the Cisco ASR1006 (RP2/FP20) Router, with IKEv2 dVTI, and the router running Cisco IOS XE 3.4 throttle builds. This could be service impacting and easily reproducible.

Workaround: Reconfigure the virtual-access interface such that the **ip nat inside** command is configured first, followed by the other commands.

- CSCtj94589

  Symptom: The Cisco ASR 1000 Router crashes when a testbed is unconfigured.

  Conditions: This issue is observed when you perform the following procedure:

  1. Configure 1000 VRF (fvrf!=ivrf).
  2. Configure one IKE session per VRF.
  3. Configure four SA duals per session.
  4. Unconfigure the testbed when the IXIA traffic ends.

  The Cisco ASR 1000 Router may crash when the **no vrf** *vrf-name* command is issued under the crypto isakmp profile.

  Workaround: There is no workaround.

- CSCtk69114

  Symptom: The RP resets when performing ESP reload, which includes crypto configuration.

  Conditions: This issue is observed when you perform the following procedure:

  1. Unconfigure and configure the interface configuration.
  2. Reload both the ESPs.

  The RP crashes on the server at the end of this procedure.

  Workaround: There is no workaround.

- CSCtl92842

  Symptom: The Cisco ASR1000 Router crashes in the controller-config mode.

  Conditions: This issue is observed when SPA-CHOC3-CE-ATM is removed and configured in the controller config mode (config-controller).

  Workaround: Exit the controller config (config-controller) mode before removing the SPA.

- CSCtn28194

  Symptom: When the virtual CEM interface is disabled, it drops out-of-band clocking packets, after an RP switchover.

  Conditions: This issue is observed when RP switchover is performed with out-of-band clocking.

  Workaround: If the network clock status changes after the standby RP is booted, execute the **shut** and **no shut** commands on the virtual CEM circuit.

- CSCtn55892

  Symptom: The CEM interface status is shown as Down on a Cisco ASR1000 Router.

  Conditions: This issue is observed upon configuring CESoPSN or the SAToP circuit on a freshly booted router. However, the traffic flow is not affected despite the CEM interface status being Down.

  Workaround: Execute the **shut** and **no shut** commands on the CEM interface in order to bring the interface up.

- CSCto09829

  Symptom: The standby ESP crashes intermittently, with FTP traffic generating a core and throwing tracebacks on the console.

Conditions: This issue is observed when the WCCP is configured along with the firewall and the FTP traffic is running.

Workaround: There is no workaround.

- CSCto16196

  Symptom: Unconfiguring and reconfiguring of WCCP tunnels results in tracebacks. The tracebacks are accompanied by partial or full traffic loss.

  Conditions: This issue is seen on the routers that have the WCCP and PFR features enabled. Reapplying the WCCP after WCCP tunnels are configured and unconfigured, causes this issue.

  Workaround: There is no workaround.

- CSCto32753

  Symptom: The old IPSec SAs cannot be removed after the DVTI client is reloaded.

  Conditions: This issue is observed when you establish 8000 IPSec SAs using the DVTI server-client mechanism. When you reload the DVTI client a couple of times, with a reload time interval of 10 minutes, the number of IPSec SAs on the DVTI server increases above 10000 and soon approaches 20000, crossing the SAs limit of 8000.

  Workaround: There is no workaround.

- CSCto76009

  Symptom: The crypto SS crashes after a clear crypto session on the DVTI client.

  Conditions: This issue is observed when you perform the following procedure:

  1. Configure 1000 VRFs.
  2. Configure one IKE session per VRF.
  3. Configure four IPSec SA duals per session.

  When you execute the **clear crypto session** command every 3 minutes on the DVTI client after all the SAs have been established, the crypto SS crashes on the DVTI server at the end of this procedure.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.3.1S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.3.1S.

- CSCtn71898

  Symptom: During an ISSU subpackage upgrade from Release 3.2.x to Release 3.3.0, the router crashes. During an ISSU subpackage downgrade from Release 3.3.0 to Release 3.2.x, the standby RP does not come up correctly after the procedure. Instead, the standby RP reloads continuously and IPC timeout messages are generated each time the RP reloads.

  Conditions: These issues are observed when ISSU subpackage upgrade is performed on the router.

  Workaround: There is no workaround.

- CSCth52252

  Symptoms: When more than one EzVPN clients initiate a connection to the dVTI EzVPN server using the same NAT device, the first client connects to the server. But when the second client connects to the server, traffic passes through the second client, but fails on the first client.

  Conditions: This issue is observed when more than one EzVPN clients initiate sessions to the dVTI EzVPN server using the same NAT device.

Workaround: There is no workaround.

- CSCtj46670

  Symptoms: The IPCP cannot be completed after the dialer interface has moved out of the Standby mode. CONFREJ is seen while negotiating the IPCP.

  Conditions: This symptom is observed when the dialer interface has moved out of the Standby mode. When a dialer debugs is enabled, the `DDR: Cannot place call, no dialer string set` error message is displayed.

  Workaround: Reload the router.

- CSCtj55624

  Symptoms: The Cisco ASR 1000 Router crashes when the **show crypto ruleset** command is run.

  Conditions: This issue is observed when the v6 crypto maps are configured.

  Workaround: Do not run the **show crypto ruleset** command.

- CSCtj78966

  Symptoms: The Cisco ASR 1000 Router crashes if many operations of IKEv2 sessions are open.

  Conditions: This symptom is seen when the IKEv2 SA DB WAVL tree gets corrupted after the SA insertion failure occurs, for example, during the PSH duplication.

  Workaround: There is no workaround.

- CSCtj87846

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

  Conditions: This issue occurs when a subinterface is used as an external interface and the corresponding physical interface goes down and comes up. The PfR master is not notified that the subinterface is up.

  Workaround: Execute the **shut** or **no shut** commands on both the PfR master and PfR border.

- CSCtj91149

  Symptoms: After the dynamic XConnect-based ISG session is up on the active RP, a delay of approximately 30 seconds is observed for the dynamic XConnect-based ISG session to be up on the standby RP.

  Conditions: This symptom occurs on switchover.

  Workaround: There is no workaround.

- CSCtj94510

  Symptoms: When sessions are being set up with the configuration of 1000 VRFs (fvrf!=ivrf)—one IKE session per VRF and four SA duals per session—a crash occurs during the Crypto_SS_process.

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

  Workaround: There is no workaround.

- CSCtk46381

  Symptoms: Service policy installation on the L2transport PVP fails when the shaping rate is changed.

  Conditions: This issue occurs when the PVPs shaping rate of the PVPs is changed.

  Workaround: Remove and reinclude the service policy.

- CSCtk83638

  Symptoms: An IP address from an incorrect pool is assigned to a client when the client reconnects with a different pool of IP addresses.

  Conditions: This issue is observed in a setup where two clients are behind a NAT router. This occurs when one client's connection is broken and the server is not aware of it, and the client reconnects with a different group and the IP address that is assigned is not from the correct pool.

  Workaround: There is no workaround.

- CSCtl70143

  Symptoms: Sometimes, the Broadband L2TP Access Concentrator (LAC) does not forward a Point-to-Point-Protocol (PPP) CHAP-SUCCESS message from the L2TP Network Server (LNS) to a client.

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

  Workaround: There is no workaround.

- CSCtl78285

  Symptoms: In a VRF configuration, an RD cannot be deleted after the RD configuration is deleted.

  Conditions: This occurs when the VRF is configured with the RD.

  Workaround: Remove the VRF configuration and add the VRF again.

- CSCtl84797

  Symptoms: An SBC traceback occurs.

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

  Workaround: There is no workaround.

- CSCtl98535

  Symptoms: The "`FMANRP_CEF-4-UPDSTATSERR: Update CEF statistics error`" traceback error message is displayed when different images are running in the active and standby RPs.

  Conditions: This occurs when different Cisco IOS software images are running in the active and standby RPs.

  Workaround: There is no workaround.

- CSCtl99266

  Symptoms: 1) CoA service login is not synchronized to the standby RP. 2) CoA multiservice login and logout are not synchronized to the standby RP.

  Conditions: The first issue occurs when a CoA service logout that was not installed through CoA service login (that is installed through a rule or as an auto service) takes place. The configuration gets synced to standby. When you perform a CoA service login of the same service.

  The second issue occurs when you perform a CoA multiservice login and logout of more than one service takes place. The services are applied or unapplied on an active RP, but not on a standby RP.

  Workaround: For the first issue, if the CoA service login is not synchronized, reboot the standby RP. After the standby RP comes up, initiate a bulk synchronization from the active RP. This synchronizes the service login. For the second issue, there is no workaround.

- CSCtn19444

  Symptoms: Both the mLACP PoAs may bundle their memberlinks, resulting in both the PoAs becoming active.

  Conditions: This issue occurs when running mLACP. The ICRM connection between the PoAs is lost. If the interface that is configured as the backbone interface also goes down on one of the PoAs, that PoA might keep its port channel memberlinks bundled. The end result is that both the PoAs are in the mLACP active state, and both have their port channel memberlinks bundled.

  Workaround: Configure 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 memberlinks to both the PoAs at the same time.

- CSCtn38996

  Symptoms: All MVPN traffic gets blackholed when a peer is reachable using a Traffic Engineering (TE) tunnel. Although an interface flap is performed so that a secondary path can be selected, the multicast route does not contain a native path that uses the physical interface.

  Conditions: This issue occurs when MPLS traffic-eng multicast-intact is configured under OSPF.

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

- CSCtn39632

  Symptoms: The RSA key cannot be configured under a key ring. It can be configured only in the global configuration.

  Conditions: This issue occurs on a Cisco ASR 1000 Series Router that is configured for RSA key encryption, with the key ring name having more than eight characters.

  Workaround: Modify the key ring name such that it is less than eight characters.

- CSCtn42601

  Symptoms: The Cisco router may unexpectedly reload when OSPF event debugging is enabled.

  Conditions: This issue is observed when you perform the following procedure:

  1. Configure the OSPF router to redistribute another protocol, with redistribution being controlled by a route map.
  2. Enable the **debug ip ospf events** command.

  Workaround: Do not reconfigure route maps when OSPF event debugging is in progress. Disable OSPF event debugging before making configuration changes to the route map.

- CSCtn46263

  Symptoms: Memory leaks are seen in ikev2_packet_enqueue and ikev2_hash.

  Conditions: This symptom is observed during retransmissions and window throttling of requests.

  Workaround: There is no workaround.

- CSCtn51058

  Symptoms: Traffic drops lead to long multicast reconvergence periods.

  Conditions: This issue is observed when stateful switchover (SSO) is performed.

  Workaround: There is no workaround.

- CSCtn51740

  Symptoms: Memory leak is observed during the EzVPN process.

Conditions: This symptom is seen when an EzVPN connection is configured with split tunnel attributes.

Workaround: There is no workaround.

- CSCtn56526

  Symptoms: In the current Cisco IOS XE 3.2.0 software, MBS is calculated based only on the MTU value. User-defined MBS value that can be calculated using the **show atm pvc** command is not displayed.

  Conditions: This issue is observed when you perform the following procedure:

  1. Configure the MBS from the command-line interface (CLI).
  2. Check the **show atm pvc** command output.

  The MBS does not reflect the configured value. It's value is always based on MTU size.

  Workaround: There is no workaround.

- CSCtn61834

  Symptoms: The NAT-T keepalive configuration is unable to send the cause for the NAT translation timeout.

  Conditions: The NAT translation table is getting timed out, because no NAT keepalive message is received.

  Workaround: There is no workaround.

- CSCtn64500

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

  Conditions: This issue is caused because of an incomplete inject P2MP multicast adjacency on the 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: Execute the **clear adjacency** command to force the repopulation of the incomplete adjacency. You should be aware of the impact of this system-wide command. Alternatively, you can use unicast commutation if it is possible to do so.

- CSCtn73941

  Symptoms: After performing an OIR for an ES+ card having EVC configuration with the **module clear-config** command, performing a restore of the old configuration is no longer functional, indicating that traffic will not be forwarded over to those service instances. The VLANs used in the previous configuration cannot be effectively used on the ports, even if the service instance numbers are changed.

  Conditions: This symptom occurs when the **module clear-config** command is configured.

  Workaround: There is no workaround.

- CSCtn74169

  Symptoms: The router crashes because of the memory corruption that occurs with the use of the EzVPN Web-intercept daemon process.

  Conditions: This issue is observed when the EzVPN connection comes up after HTTP authentication is completed with the help of the HTTP intercept.

  Workaround: HTTP intercept should not be used.

- CSCtn80993

  Symptoms: After performing an OIR of a SPA, the Cisco IOS crashes.

Conditions: This issue is observed when you perform the following procedure:

1. The router has scaled the L2VPN configuration of 7000 EoMPLS.
2. The router is configured with 1500 TE tunnels, 6000 EVC, and 3000 L2TPV3 sessions.
3. A SPA OIR is performed, when the traffic is passing through the sessions.

The Cisco IOS crashes consistently after these configuration steps are performed.

Workaround: After the SPA comes up, wait for 1 minute before issuing the second reload.

- CSCtn81231

  Symptoms: Multicast traffic is not forwarded out of the RBE interface because of incomplete multicast adjacency.

  Conditions: This issue is observed when you perform the following procedure:

  1. An ATM DCHP host running IGMPv2 is established over the RBE interface of the router.
  2. Multicast group join configuration is successful.

  However, multicast adjacency is incomplete and hence cannot forward multicast traffic.

  Workaround: Execute the **shut** command followed by the **no shut** command on the ATM main interface.

- CSCtn87155

  Symptoms: The CoA sessions do not come up.

  Conditions: This symptom is seen when some CLI commands are called within the shell function. The CLI commands may fail if the shell programatic APIs are used.

  Workaround: Manually use the shell function on the console.

- CSCtn98642

  Symptoms: The ASR RP crashes with the: `UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Ether-SPA background process` error message.

  Conditions: This issue is observed when you perform the following configurations:

  1. Perform a large-scale configuration having QinQ and QinQ-Any with the same outer VLAN on the SPA.

  Note Configuration of QinQ (min 50) and QinQ-Any with the same outer VLAN is mandatory.

  2. Reload the router.

  Workaround: There is no workaround.

- CSCto00318

  Symptoms: Performing an SSH on an existing SSH session causes the router to reboot at times.

  Conditions: This issue is observed when an intermediate server is an IOS server. An SSH session initiated from a router running Cisco IOS Release 15.x IOS may cause the router to reboot. Do not initiate an SSH session from the Cisco router running the Cisco IOS 15.x IOS release train.

  Workaround: There is no workaround.

- CSCto02448

  Symptoms: The AS Path attribute is lost when performing an inbound route refresh.

Conditions: This symptom is observed when you perform the following procedure:

1. Configure the neighbor with soft reconfiguration inbound.
2. Do not configure the inbound route map for the neighbor router.

The nonroute map inbound policy (filter-list) allows the AS path.

Workaround: Instead of using the nonroute map inbound policy, use the route map 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

- CSCto44585

  Symptoms: Packets with the DF-bit set across the L2TPV3 tunnel are punted or dropped into the CPU.

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

  Workaround: Reduce the size of the MTU on the client side.

- CSCto48592

  Symptoms: The IPFRR: IOS crashes when switchover is performed.

  Conditions: This issue is observed when you perform the following procedure:

  1. Enable IPFRR.
  2. Enable BFD.
  3. Perform a switchover to the active RP.

  Workaround: There is no workaround.

- CSCto52235

  Symptoms: The **mac address accounting** command is missing in the Cisco ASR 1000 Router.

  Conditions: Not applicable.

  Workaround: There is no workaround.

- CSCto63954

  Symptoms: The router crashes continuously, if GETVPN is configured in the router.

  Conditions: This symptom occurs when GETVPN-related configuration is performed in the router.

Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.3.0S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.3.0S.

- CSCti53718

  Symptom: While performing a consolidated package upgrade on the Cisco ASR 1006 Router, the standby ESP does not proceed beyond the Init state.

  Conditions: This issue is observed in active PPPoEoA sessions when a create-on-demand VC with no PPP keepalive is configured and QoS is configured at the BB session level.

  Workaround: Configure a PPP keepalive.

- 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

- CSCtj31320

  Symptom: MLP bundles miss adjacencies after a scaled configuration router is reloaded. The bundles either do not process traffic or process only traffic that is forwarded in one direction. When the **show ip route** command is run, the output indicates that there is no adjacency entry for the peer IP address.

  Conditions: This issue is observed after the router is reloaded, a hardware OIR is performed, an interface flaps, or some other event that causes a large number of MLP bundle sessions to be terminated and re-established occurs.

  Workaround: For MLP over Serial interfaces, perform one of the following actions on the bundle:

  - Run the **clear interface** *bundle_interface_name* command.
  - Shut down, and then restart the bundle.

  For MLPPPoE interfaces, run the **clear interface** *bundle_interface_name* command.

  The bundle may recover after you perform one of these actions. In addition, to avoid this issue if flaps occur in the future, implement the following combination of PPP and multilink options:

  - ppp timeout retry 4
  - ppp max-failure 30
  - ppp multilink ncp sequenced never

- CSCtk03524

  Symptom: Applying a single dynamic crypto map to a large number (for example, 2000) of subinterfaces while the crypto session is being set up causes the `iosd check heap coredump` error.

  Conditions: This issue is observed when a large number of subinterfaces share a single dynamic crypto map.

  Workaround: Configure each subinterface to use a different crypto map.

- CSCtk10772

  Symptom: The LNS CPS rate is reduced for PPP/VPDN sessions.

  Conditions: This issue is observed when LNS is configured with dual RP in SSO High Availability mode. The LNS CPS rate is reduced when the session count exceeds 16000 PPP/VPDN sessions.

  Workaround: Disable SNMP on the virtual-template by running the **no virtual-template snmp** command.

- CSCtk69937

  Symptom: Packets may get dropped during the IPSec rekey process in an IKEv2 session.

  Conditions: This issue is observed during the IPSec rekey process in an IKEv2 session.

  Workaround: There is no workaround.

- CSCtl71869

  Symptom: A traceback is seen when the **default interface** command is run using a script to clean up the configuration on the interface.

  Conditions: This issue is observed when an Ethernet service instance (that is, the EFP) is configured on the interface.

  Workaround: Manually run the **default interface** command. If you want to include the command in a script, then add a delay in the script before the command is run.

- CSCtl92842

Symptom: The router crashes if SPA-CHOC3-CE-ATM is removed while the router is being configured in the Controller Configuration mode.

Conditions: This issue is observed when SPA-CHOC3-CE-ATM is removed while the router is being configured in the Controller Configuration mode.

Workaround: Exit the Controller Configuration mode before removing the SPA.

- CSCtl95778

  Symptom: BBA traffic is dropped on the standby RP while an ISSU upgrade from Cisco IOS XE Release 3.1.x or 3.2.x to 3.3.0 is in progress. In addition, L2TPv3 traffic is lost and cannot be recovered after the ISSU is completed.

  Conditions: This issue is observed when an ISSU is performed from Cisco IOS XE Release 3.1.x or 3.2.x to 3.3.0.

  Workaround: Manually reload the standby RP before the final RP switchover.

- CSCtl99266

  Symptom: The following issues related to CoA services are observed:

  - CoA service activation details are not propagated from the active RP to the standby RP.
  - CoA multiservice activation or deactivation of multiple services is not propagated from the active RP to the standby RP.

  Conditions: The first issue is observed when the following steps are performed:

  1. Perform a CoA service deactivation of a service that was not installed though CoA service activation (that is, it was installed through a rule or as an auto service). The deactivation details are propagated to the standby RP.
  2. Perform a CoA service activation of the same service. The activation details are not propagated to the standby RP.

  Workaround: For the first issue, reboot the standby RP. There is no workaround for the issue related to CoA multiservice activation or deactivation.

- CSCtn00790

  Symptom: PPPoEoA sessions are not automatically re-established after an RP switchover.

  Conditions: This issue is observed when ISG is configured.

  Workaround: There is no workaround.

- CSCtn28194

  Symptom: After an RP switchover, the virtual-cem interface is disabled and drops out-of-band clocking packets.

  Conditions: This issue is observed when an RP switchover is performed with out-of-band clocking.

  Workaround: If the network clock status changes after the standby RP is started, shut down and then restart the virtual-cem circuit.

- CSCtn28453

  Symptom: The virtual-cem interface remains in the down/down state. This results in packets getting dropped because of input errors.

  Conditions: This issue is observed when `system` is configured as the source of the network clock by using the **network-clock select** *priority* **system** command and is selected as the active source, but is not selected for CEM out-of-band clocking.

  Workaround: There is no workaround.

- CSCtn31692

  Symptom: After an RP switchover, the BITS clock is not selected as the ACTIVE clock source. Instead, the system clock is selected as the ACTIVE clock source.

  Conditions: This issue is observed when a valid BITS clock source is connected to R0 or R1, the network clock is configured using the **network-clock select** *priority* **BITS** *R0/R1* command to select BITS input from R0 or R1, and an RP switchover is performed.

  Workaround: There is no workaround.

- CSCtn43861

  Symptom: When the parameterized L4R-Whitelist combo service is applied, incoming packets matching the whitelist may still get redirected. In addition, explicit traffic priorities configured in the service template are not inherited by the parameterized service policy. When the **show subscriber session uid** *uid* is run, the priorities configured for the services are not correctly displayed.

  Conditions: This issue is observed when the **show subscriber session uid** *uid* command is run. However, note that after explicitly applying a priority to the parameterized L4R and the whitelist TCs, if you try service activation either through Access-Accept or CoA, the sessions come up and the services are activated.

  Workaround: There is no workaround.

- CSCtn44232

  Symptom: When multiple RP switchovers are performed, a stage may be reached where both RPs are unusable.

  Conditions: This issue is observed when multiple RP switchovers are performed.

  Workaround: There is no workaround.

- CSCtn55892

  Symptom: The CEM interface is in the down/down state.

  Conditions: This issue is observed when you configure a CESoPSN or SAToP circuit on a recently booted router. Note that traffic flow is not affected because of this issue.

  Workaround: Shut down, and then restart the CEM interface.

- CSCtn62287

  Symptom: The standby RP may crash while flapping the interface or 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.