Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8S

This chapter provides information about the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8S.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8.2S

This section describes the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8.2S. It contains the following topics:

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.8.2S

This section documents the unexpected behavior that might be seen in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8.2S.

- CSCtq81245

  Symptom: SPA-4XCT3/DS0 reloads after performing an fp reload.

  Conditions: 1. Issue is seen on a single fp system 2. Issue is seen when serial interfaces are configured on the SPA.

  Workaround: There is no workaround.

- CSCuc47356

  Symptoms: Static routes are not getting removed.

  Conditions: This symptom is observed with Smap - Smap. Removal of CLI does not remove the static route.

Workaround: Remove the ACL before removing the SA.

- CSCuc65049

  Symptoms: Routing might not be in accordance with the performance routing policy even when NBAR classifies packets correctly.

  Conditions: This may occur after reloading a Performance Routing (PfR) configuration onto the router.

  Workaround: When links between routers are defined by OSPF (Open Shortest Path First), the problem does not occur. Use the recommended PfR configuration, using OSPF, to define peers for each border router.

- CSCud14945

  Symptom: IPv4 IP Security (IPSec) tunnel bring up time is longer in the dynamic crypto-map deployment.

  Conditions: This symptom is observed on a Cisco ASR1000 series router that functions as an IPSec termination and aggregation router.

  Workaround: There is no workaround.

- CSCud24378

  Symptom: Traffic rate verification fails after QoS configuration changes.

  Conditions: On QoS configuration changes, after re-adding the p-map on tunnel.

  Workaround: There is no workaround.

- CSCud64870

  Symptom: DMVPN hub ASR1004 may crash after the fetching CRL from MS CRL server.

  Conditions: The crash occurs when there are 5 CDPs for the hub router to fetch the CRL. Since there are multiple CDPs, the hub router fetches the CRL in a parallel way, which leads to a crash under a timing issue.

  Workaround: Setting up one CDP instead of multiple CDPs will avoid the timing condition that leads to the crash.

- CSCud77549

  Symptom: CPPOSLIB-3-ERROR_NOTIFY error messages are reported while trying to configure the inspect policy for the ZBF in ASR1K.

  Conditions: ZBF config, good number of entries in the ACL maps under the class-map

  Workaround: Reload the ESP and remove the ACL entry that is creating the issue.

- CSCue48456

  Symptom: Call is disconnected after CUBE sends **BYE** to both call legs.

  Conditions: Occurs on a video call where a mid-call re-INVITE occurs to modify the media stream.

  Workaround: There is no workaround.

- CSCue50255

  Symptom: ucode crashes at `REM_REM_MISC_ERR_LEAF_INT_INT_REM_POP_REQ_TO_EMPTY_SCHE`

  Conditions: on flapping multilink interfaces

  Workaround: There is no workaround.

- CSCue51375

  Symptom: The dynamic monitor is populated with incorrect records and the performance monitor cache incorrectly includes encapsulated traffic.

  Conditions: This issue might occur when a GRE tunnel output interface is configured with a performance monitor on an ASR1000 series router, and the output physical interface from which the packets are transmitted is configured with a native FNF monitor.

  Workaround: There is no workaround.

- CSCue53207

  Symptom: A record that contains certain derived fields (listed below) may be punted incorrectly to the route processor (RP) and lost.

  Conditions: Records can collect “derived” fields; calculating derived fields is dependent on the values of other fields. The fields listed below are incorrectly defined as derived and dependent on other fields. When a record contains one of these fields and does not include its dependent fields, the record is punted to the route processor (RP) to complete the record processing. Punting these records might lead to record loss.

  Workaround: When configuring a monitor to collect one of the fields listed below, collect each of the dependent fields also. The list indicates the dependencies:

  - “connection delay application sum” is dependent on:

    connection delay response to-server sum

    connection delay network to-server sum

    connection server response sum
  - “connection delay application min” is dependent on:

    connection delay response to-server min

    connection delay network to-server sum
  - “connection delay application max” is dependent on:

    connection delay response to-server max

    connection delay network to-server sum
  - “connection delay response client-to-server sum” is dependent on:

    connection delay response to-server sum

    connection delay network to-server sum

    connection server response sum
  - “connection delay response client-to-server min” is dependent on:

    connection delay response to-server min

    connection delay network to-server sum

    connection server response sum

    connection delay response to-server sum

    connection delay network to-server min.
  - “connection delay response client-to-server max” is dependent on:

    connection delay response to-server max

    connection delay network to-server sum

connection server response sum

connection delay response to-server sum

connection delay network to-server max

- CSCue80506

  Symptom: Traceback at DMVPN Spoke registration, DMVPN QoS policy not deployed to QFP datapath component.

  Conditions: DMVPN, NHRP, QOS.

  Workaround: There is no workaround.

- CSCuf04726

  Symptom: With IPsec (crypto-map mode) configured, after VFR disable followed by ASR reboot, the **no ip virtual-reassembly-out** CLI is lost and VFR is re-enabled.

  Conditions:

  1. Apply crypto map on the interface.

  2. Manually disable VFR with the **no ip virual-reassembly-out** command.

  3. Save config.

  4. Reload.

  Workaround: After reload, again disable VFR with **no ip virual-reassembly-out**.

- CSCuf20409

  Symptom: Netsync customer seeing clock in ql-failed state on one ASR-2ru.

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

  Workaround: If both SPAs are in the same slot, do not send the secondary config.

- CSCuf43548

  Symptom: When POS Rx fiber at the tail end of the MPLS TE FRR is pulled, the FRR takes longer than 200 ms to cut over to the other Tunnel.

  Conditions: This happens with POS MPLS TE FRR, when head end receives remote defect due to rx fiber pull at the tail end. Remote defects wont trigger FRR quickly.

  Workaround: There is no workaround.

- CSCuf50092

  Symptom: Flow Around is not working with a 3.8 CCO image.

  Conditions: This issue is seen only on 3.8 CCO image and not in 3.8 throttle pull image.

  Workaround: There is no workaround.

- CSCuf61531

  Symptom: Under load condition with contact-center call flows, some calls might be disconnected unexpectedly. ASR CUBE is sending unexpected **BYE** for a single call for VZ call flow

  Conditions: Load of 40 CPS in a contact-center flow, multiple SIP messages with DSP, and call-block feature.

  Details: VZ business call flow, where multiple mid-call re-invites with insertion and deletion of transcoder in the call. Call block is enabled, so no mid-call changes are sent over ISP network.

  Workaround: There is no workaround.

- CSCuf65404

  Symptom: A call fails if the transcoder is needed for DTMF interworking and vcc offer-all is configured.

  Conditions: CUBE reserves the transcoder for codec mismatch and releases the transcoder, since the codecs are identical. But dtmf still requires the transcoder for interworking.

  Workaround: There is no workaround.

- CSCuf65537

  Symptom: Crash with Verizon contact-center call flow.

  Conditions: Crash is observed with CAC configs & 40 cps call rate:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = RSCCAC CALL DENIAL SCAN
  -Traceback= 1#0ac7b601f45270393178c559213c70ba  :400000 344C0D0 :400000 699DCD1
  :400000 344C43B :400000 344C386 :400000 344C6B0 :400000 699D248
  ```

  Workaround: There is no workaround.

- CSCuf74266

  Symptom: ASR-CUBE: Crash observed with DSMP.

  Conditions: Load scenario issue is observed.

  Workaround: There is no workaround.

- CSCug04450

  Symptom: PfR fails to control traffic-classes when the subnet mask is greater than the prefix length.

  Conditions: The issue is seen either with the default prefix length or when the prefix length is configured.

  Workaround: Configure aggregation-type as BGP instead of prefix-length.

- CSCug08561

  Symptom: After a Web logon, the user does not get a Web logon response page sent by the portal. If the Web logon is successful, the user is not redirected to the Web address specified. Instead, the user is redirected to the portal for authentication.

  Conditions:

  1. Walkby feature is enabled with L4R & PBHK features applied to lite session.

  2. User initiated the Web logon request.

  Details: Upon a Web logon, an account-logon **COA** request is triggered from the portal to ISG. In ISG, the request triggers conversion of the lite session to a dedicated session. During the conversion, lite session and its associated resources (L4R and PBHK mappings) are removed from PD, and the dedicated session gets provisioned. Once conversion is done, ISG replies to the portal with **COA ACK/NACK**. Based on the response from ISG, the portal generates a Web logon response-page (**SUCCESS/FAILURE**) and sends it back to the client.

  But when the response packet reaches ISG, it does not get classified to the downstream session (because PBHK & L4R mapping were deleted). As a result, the packet is dropped in ISG.

  Workaround: There is no workaround.

- CSCug12997

  Symptom: The ASR 1004 router crashes with:

  ```
  CPPHA-3-FAULT: F0: cpp_ha:  CPP:0.0
  desc:ETC_ETC_LOGIC1_LEAF_INT_INT_LP_LONG_PKT_ERR det:DRVR(interrupt) class:OTHER
  sev:FATAL id:2694 cppstate:STOPPED res:UNKNOWN flags:0x7 cdmflags:0x0
  ```

Conditions: VASI, cryto, mpls, during normal operation (as per what is known).

Workaround: There is no workaround.

- CSCug21859

  Symptom: With NBAR configured on the NAT interface, an ASR1000 crashes on receiving a broken packet.

  Conditions: ASR1000 DNS packet coming (broken at L4 header), NBAR configured (**match protocol dns**), NAT with vasi interfaces.

  Workaround: There is no workaround.

- CSCug27334

  Symptom: ASR router might start using new SPIs before quick mode exchange finishes. This causes invalid SPI messages on the receiver side and, in some cases, flap of IKE/IPsec.

  Conditions: First seen on IOS XE 15.2(4)S with DMVPN.

  Workaround: There is no workaround.

- CSCug28249

  Symptom: The ASR1004 crashes on ESP when enabling NAT. In both of the cores, the packet in question is a DNS packet. The crash is observed when trying to invoke the DNS ALG.

  Conditions: Enabling NAT causes ESP to crash

  Workaround: There is no workaround.

- CSCug28904

  Symptom: Router deops ESP packets with CRYPTO-4-RECVD_PKT_MAC_ERR.

  Conditions: Peer router sends nonce with length 256Bytes

  Workaround: There is no workaround.

- CSCug34822

  Symptom: ESP might crash.

  Conditions: While running **clear ip nat translations *** after the forced removal of a NAT mapping.

  Workaround: *Before* removing any NAT mappings, run **clear ip nat trans ***. And do *not* use the **forced** option when removing a NAT mapping. The following is an OK example:

  ip nat inside source list 1 pool pool1 overload

- CSCug37490

  Symptom: VA leak is seen when removing and reapplying a virtual template from the ISAKMP profile and clearing the crypto session. This results in a stale VA that is up, down and cannot be cleared.

  Conditions: When making changes to a virtual template under the ISAKMP profile with client session UP-IDLE (Phase 1 only, as no VT exists).

  Workaround: Reload.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.8.2S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8.2S.

- CSCtc17240

  Symptom: Some third party SIP PBXs may have interoperability problems with the authentication header of a Cisco SIP gateway.

  Conditions: Per RFC 3261 section 25.1, the **nc** value, or **nonce-count**, should have lower case hex. This is defined as follows:

  ```
  nonce-count = "nc" EQUAL nc-value
  nc-value = 8LHEX
  LHEX = DIGIT / %x61-66;lowercase a-f
  ```

  A snippet of the offending message:

  ```
  ... cnonce="305EE7FF",qop="auth",algorithm=MD5,nc=0000000A
  ```

  Workaround: There is no workaround.

- CSCtg13667

  Symptom: `Packet_Too_Big (type 2, code 0) and Destination Unreachable Administratively (type 1, code 1)` is not sent back if packets are hitting MTU checking or ACL deny on egress interface.

  Conditions: Issue is observed on ASR1000 running 15.0(01)S code.

  Workaround: There is no workaround.

- CSCts83413

  Symptom: While configuring Classic Netflow (and possibly Flexible Netflow) for export of records to a user-specified VRF, occaisionally user configuration can get out of sync or invalid. In such a case, the QFP Processor does not have the same VRF information as the IOS config. This results in Netflow export not working.

  Conditions: When this was observed, probably multiple cycles of VRF configuration as well as multiple cycles of Netflow export destinations had taken place. The endpoint was that the IOS config was to export to a particular VRF (VRF "BLUE" for example), while the QFP processor had a configuration to export to the default VRF. Thus the configuration was out of sync and Netflow export did not function.

  Workaround: Unconfigure the Netflow export destination and to reconfigure it.

- CSCtv93326

  Symptom: Inconsistency between IOS CLI and platform state with regard to flow record configuration on the router. Reporting of Mediatrace statistics may fail, with the following error reported on the Mediatrace Initiator device: `Metrics Collection Status: Fail (19, No statistic data available for reporting)`

  Conditions: This is a Flowdef modify event as a result of event consolidation. It can occur in the following scenario: 1. Detach the flowdef associated with a monitor. 2. Change the flowdef (add / delete fields). 3. Re-attach the flowdef to the monitor. For the Mediatrace symptom, the problem can occur when a route change occurs for the traffic being monitored.

  Workaround: There is no workaround.

- CSCtw74598

Symptom: Call Menu (CM) tone may be detected and suppressed in the following call Flow: Modem - - [FXS] - - VG224 - - [MGCP] - - CUCM - - [SIP] - - CUBE - - [SIP] - - PSTN Modem connected to the VG224 places an outbound call to a destination in the PSTN. CM tone from the originating modem gets removed by the VG224. To verify the symptom, enable "debug voip hpi notification" and you would see a line "MODEM CM tone detected" in the debug output.

Conditions: SIP trunk provider does not support NSE based modem passthrough and hence VG224 was not configured with "mgcp modem passthrough".

Workaround: 1. Configure the FXS port as a non-mgcp port, disable fax relay and sg3-to-g3 suppression commands at the voip dial-peer level : dial-peer voice 99920 pots no service mgcpapp port 2/0 dial-peer voice 4001 voip destination-pattern 4001 session protocol sipv2 session target ipv4:<ip-address> codec g711ulaw no fax-relay sg3-to-g3 fax protocol none no vad 2. Downgrade to 15.1(3)T4.

- CSCty59423

  Symptoms: Memory leak seen with following messages:

  ```
  Alternate Pool: None  Free: 0  Cause: No Alternate pool

  -Process= "VOIP_RTCP", ipl= 0, pid= 299

  -Traceback= 0x25B1F0Cz 0x25AB6CBz 0x25B1029z 0x46C02Ez 0x46C89Bz 0x46BCC2z 0x471D12z
  0x43EF59Ez 0x43DD559z 0x43DCF90z

  %SYS-2-MALLOCFAIL: Memory allocation of 780 bytes failed from 0x46C02E, alignment 32
  ```

  Conditions: The conditions are unknown.

  Workaround: There is no workaround.

- CSCty94210

  Symptom: IKEv2 CERTREQ payloads exchanged by initiator and responder both contain all trustpoints and trustpools. This enhancement request is for limiting the size of the CERTREQ payload based on the configuration (global for responder, IKEv2 profile for initiator).

  Conditions: None.

  Workaround: There is no workaround.

- CSCua78782

  Symptom: Authentication of EzVPN fails.

  Conditions: The symptom is observed with BR-->ISP-->HQ.

  Workaround: There is no workaround.

- CSCub06422

  Symptom: Call flow: PSTN---pri---Voice Gateway---sip---SIP server After running fine for 6-7 days, then 100% of the calls through the voice gateway fail. On a call that comes in through the PRI, INVITE is sent with `m=audio 0`. Then, on getting `200 OK` from the other end, the gateway disconnects the call.

  Conditions: Router up and running for 6-7 days.

  Workaround: Reload the router.

- CSCub19185

  Symptoms: Path confirmation fails for a SIP-SIP call with IPV6 enabled.

  Conditions: This symptom occurs when UUTs are running Cisco IOS Release 15.2(2)T1.5.

  Workaround: There is no workaround.

- CSCub35268

Symptom: Call dropping issue was found while testing new network based features on AT&T's FlexReach network. The features are network-based Simultaneous Ringing and Sequential Ringing.

Conditions: The following is the behavior for Simultaneous Ringing: 1. Hopon call from PSTN to 7323204351 2. Both Phone 2 (7323204351) and Phone 3 (7323204350) ring 3. Phone 3 is answered, but immediately drops 4. Phone 2 stops ringing (I see CANCEL from AT&T for this call-id) 5. PSTN caller continues to hear ringback tone Per the attached trace, CUBE fails to send a 200 OK with SDP in response to AT&T's re-INVITE to open up the voice channel. For Sequential Ringing: 1. HOPON from 4085271217 (Phone 1) to Phone 3 (7323204350) 2. Note the INVITE has media attribute codec pref 18 0 100 ; INACTIVE 3. CUBE sends 100 Trying then 180 Ringing 4. Phone rings ~3X then call is cancelled by AT&T side by sending SIP CANCEL message 5. CUBE acknowledges by sending 200 ok followed by 487 Request Cancelled 6. AT&T sends INVITE to Phone 2 (7323204351) with media attribute codec pref 18 0 100 ; INACTIVE 7. CUBE sends 100 Trying then 180 Ringing 8. Upon answer - CUBE sends 200 ok with no codec pref in media attribute 9. AT&T sends re-INVITE - with no SDP 10. CUBE sends 100 Trying 11. AT&T sends BYE even before CUBE can send 200 ok 12. Caller from AT&T side hear continuous RINGBACK tone Again, per the attached trace on Sequential Ringing, CUBE fails to send a 200 OK with SDP in response to AT&T's re-INVITE to open up the voice channel. Per AT&T, their side might be sending the BYE because CUBE sends its initial 200 OK with SDP but no codec preference. (refer to Sim. Ring Trace).

Workaround: There is no workaround.

- CSCub53856

  Symptom: On ASR1K and related platforms, when configuring a Flow NetFlow (FNF) Performance Monitor with a record that has a large number of fields (typically 30 or more), the following traceback may be observed at the time that the Service Policy is bound to the interface:
  `%FNF-3-FNF_FIELD_LIST_TOO_LARGE: Field_list too large, max 32.`

  Conditions: Configuring a Performance Monitor, typically with more than 30 fields, and binding it to an interface via a Service Policy.

  Workaround: Reduce the number of fields. Using fewer than 30 should work, although it does depend on the exact fields in the record.

- CSCub63208

  Memory corruption detected in memory, when allocated for RTCP statistic

  Symptom: An error occurs when CALL_CONTROL-3-STAT_MEMORY_CORRUPTED: Memory corruption detected in memory=XYZ allocated for RTCP statistic.

  Conditions: This condition is occurs when call involves trans-coding.

  Workaround: There is no workaround.

- CSCub86827

  Symptom: To enable CFA to 918079611, then press 'CFwdALL' softkey and enter any 4 digit number, then enter 918179611 and press end. After this we will be able to see "Forwarded to 918179611" on Phone.

  Conditions: This condition is observed when SRST mode is configured with after hours.

  Workaround: Remove the after hours configuration .

- CSCub98357

  Symptom: A Cisco router running IOS-XE release 3.6.0S, IOS release 15.2(4)M or newer may reload.

  Conditions: This condition is observed during key exchange with OCSP disable nonce configured.

Workaround: Disable 'ocsp disable-nonce'.

- CSCuc12685

  Symptom: Address Error exception is observed with **ccTDUtilValidateDataInstance**.

  Condition: This symptom is observed with **ccTDUtilValidateDataInstance**.

  Workaround: There is no workaround.

- CSCuc22348

  Symptom: 3900e running 15.2(3)T1 crash at **be_MediaOper_UpdateStats**

  Condition: 3900e running 15.2(3)T1 crash at **be_MediaOper_UpdateStats**

  Workaround: There is no workaround.

- CSCuc27517

  Symptom: Permanent license disappear after the IOS upgrade or downgrade.

  Conditions: This symptom occurs when:

  - The ASR1001 IOS is upgraded from 03.05.02 or older to 03.06.00 or later.
  - The IOS is downgraded from 03.06.00 or later to 03.05.02 or older.

  Workaround: Without this fix: Do a license save from 3.4 before the upgrade and re-install in 3.6 in 34, save all the licenses to a file to bootflash **1RU#license save <file location>** in 36 , install back all the licenses from the file **1RU#license install <file location>.**

  With this fix: To avoid this, customers have to create a file in the bootflash called **1RU_34_36_ENFORCE_LICENSE_MIGRATION** to enforce the migration of all the licenses before the upgrade process. The file will be removed automatically after the license migration.

  For example: **1RU#license save bootflash:1RU_34_36_ENFORCE_LICENSE_MIGRATION** For the routers, which are already experiencing this issue, customers can either try to reinstall the licenses or downgrade to 34, create the file in bootflash and upgrade with 36 or later image with this fix again.

- CSCuc39418

  Symptom: When IKE sends `KEY_MGR_CLEAR_ENDPT_SAS` during initial contact, IPSec sends `KEY_ENG_DELETE_SAS`.

  Conditions: on performing SSO in spoke.

  Workaround: There is no workaround.

- CSCuc40912

  Symptom: Stale objects are seen on RP SWO.

  Conditions: Delete IPv6 VRF tunnel that have FNF configured and then do rpswo.

  Workaround: There is no workaround.

- CSCuc42518

  Symptom: Cisco IOS Unified Border Element (CUBE) contains a vulnerability that could allow a remote attacker to cause a limited Denial of Service (DoS). Cisco IOS CUBE may be vulnerable to a limited Denial of Service (DoS) from the interface input queue wedge condition, while trying to process certain RTCP packets during media negotiation using SIP.

  Conditions: Cisco IOS CUBE may experience an input queue wedge condition on an interface configured for media negotiation using SIP when certain sequence of RTCP packets is processed. All the calls on the affected interface would be dropped.

Workaround: Increase the interface input queue size. Disable Video if not necessary.

- CSCuc46087

  Symptoms: CUBE does not send a response to an early dialog UPDATE in a glare scenario.

  Conditions: This symptom occurs when CUBE receives an early dialog UPDATE when it sends 200OK to INVITE and expects ACK.

  Workaround: There is no workaround.

- CSCuc49319

  Symptom: An INVITE that contains a Replaces: header and also a parameter in the Request URI will be responded to with a SIP 481 Call Leg/Transaction Does Not Exist. The transfer that was the trigger of the INVITE with the Replaces: header will fail to complete.

  Conditions: This was seen on CUBE when handling a triggered INVITE during a REFER based transfer.

  Workaround: There is no workaround.

- CSCuc51076

  Symptom: The Reason: header in a SIP BYE may not be consistently passed from the incoming call-leg to the outgoing call-leg.

  Conditions: This was seen on CUBE running 15.1(4)M through 15.2(4)M1.

  Workaround: There is no workaround.

- CSCuc59979

  Symptom: The ASR drops the original media stream before the mid call is acknowledged. After the FAX negotiations fail, the ASR does not return/continue to the original media characteristics.

  Conditions: Voice to Fax switchover and remote end point do not support fax, so it responds with 488. CUBE does not update call type to voice after 488.

  Workaround: There is no workaround.

- CSCuc62078

  Symptom: **Call Flow:** 9971 ---- SIP ---- CUCM ---- SIP ---- CUBE ---- SIP ---- Provider

  Issue: Provider does not support video codecs, as soon as an INVITE with video codes in the SDP, provider is disconnecting the call. The customer wants to use Video capability for internal calls and when external call is made, is requesting if they can strip the Video attributes from SDP going in the INVITE to provider.

  Conditions: Created voice class sip-profiles 1000 and applied under the outgoing dial-peer to provider. Voice class sip-profiles 1000 request INVITE sdp-header Video-Attribute remove request INVITE sdp-header Video-Media modify "m=video(.*)" request INVITE sdp-header Video-Bandwidth-Info remove Before applying the profile, below is the snippet of SDP rcv on CUBE: After applying the profile, the SDP is like below:

  v=0 o=CiscoSystemsSIP-GW-UserAgent 1127 4805 IN IP4 10.59.0.6 s=SIP Call c=IN IP4 10.59.0.6 t=0 0 m=audio 17800 RTP/AVP 8 101 c=IN IP4 10.59.0.6 a=rtpmap:8 PCMA/8000 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 a=ptime:20 c=IN IP4 10.59.0.6.

  To remove the third c= line, tried the below under sip-profiles: not working as expected: request INVITE sdp-header Video-Session-Info REMOVE***Trying to add this line, to see if it will make any difference, however show run, displays **Video-Session-Name** request INVITE sdp-header Video-Connection-Info REMOVE***Trying to add this line, to see if it will make any difference, however **show run**, displays **request INVITE sdp-header remove**.

Workaround: If the customer does not have a requirement to have video for external calls, then much better option is to disable video at CUCM only for external calls. This can be done on CUCM by the following ways:

1. Create a new region on CUCM with video disabled.
2. Keep the SIP trunk to CUBE in that new region.
3. This way, internal calls can still have video, and there won't be any video coming to CUBE for external calls.

- CSCuc63246

  Symptom: Call Flow: PSTN->PRI->Voice GW->SIP->CUCM->IP phone. During an active call between PSTN and IP phone (non-secure), if the IP phone user presses the **Hold** key for second time call gets disconnected. **Hold** and **Resume** for the first time works fine. MOH server is using SRTP. Also, if the IP phone used is secure (SRTP), then call will not get disconnected; no matter, how many times the user presses the **Hold** and **Resume** keys. Customer has mixed mode cluster.

  Conditions: When audio session between IP phone and VG is RTP and then the **Hold** key is pressed for the second time. The MOH uses Secure RTP.

  Workaround: There is no workaround.

- CSCuc69342

  Symptoms: About 10 minutes after CUBE boot, the router crashes with the following traceback: Traceback= 5B01805 46158ED 45F4F57 45BB19E 45BA1CF 451D6DC 4525549 45252D9 4519C30 45196A9 4778FFD. After the reload from the crash, it may take sometime before it crashes again.

  Conditions: This symptom occurs when CUBE receives the SIP REFER message with the Refer-To header having no user part.

  Workaround: There is no workaround.

- CSCuc71379

  Symptom: An incoming INVITE that is received by CUBE with a Replaces: header will dropped that Replaces if the outgoing INVITE must hunt through multiple outbound dial-peers.

  Conditions: This was seen on CUBE in a SIP to SIP configuration running 15.2(4)M1.10

  Workaround: There is no workaround.

- CSCuc71735

  Symptom: A CUBE running the anti-trombone feature might fail to return SIP SDP contents in a 200 OK message on the original, incoming call leg if the outbound leg failed and was retried.

  Conditions: This was seen on CUBE running 15.2(4)M1.10 when handling calls for a SIP proxy in a "proxy-on-a-stick" type configuration (i.e. incoming / outgoing call legs all go through one CUBE).

  Workaround: There is no workaround.

- CSCuc76298

  Symptoms: In ASR B2B HA setup, the new active router crashes at ccsip_send_ood_options_ping immediately after switchover with OOD OPTIONS enabled.

  Conditions: This crash is seen in the following scenarios:

  – Standby router has OOD OPTIONS enabled either because it is present in startup configuration or enabled after boot-up.

  – Disable OOD OPTIONS.

  - When Switchover happens.

  Workaround: Reload standby router once after OOD OPTIONS configuration changes from enabled to disabled.

- CSCuc85157

  Symptom: The packet is dropped with the reason **NatIn2out.**

  Conditions: This symptom is observed due to the PAT.

  Workaround: There is no workaround.

- CSCuc85319

  Symptom: RP is crashed.

  Conditions: This symptom is observed after flapping the ATM sub-interface that is configured with the ATM bundle 8192 times

  Workaround: There is no workaround.

- CSCuc96631

  Symptoms: Incoming calls through e1 r2 stop working in Cisco IOS Release 15.2(4)M1.

  Conditions: This symptom is observed with incoming calls through e1 r2 in Cisco IOS Release 15.2(4)M1. Outgoing calls work fine.

  Workaround: Use Cisco IOS Release 15.2(2)T.

- CSCud08595

  Symptoms: After the reload, ISDN layer 1 shows as deactivated. **Shut** or **no shut** brings the PRI layer 1 to Active and multiframe is established in layer 2.

  Conditions: This symptom occurs when **voice-class busyout** is configured and the controller TEI comes up before the monitored interface.

  Workaround: Remove the **voice-class busyout** configuration from the voice-port.

- CSCud19536

  Symptom: In AVC for IOS XE 3.8, a short downtime is experienced after modifying the AVC configuration.

  Conditions: The symptom is observed when removing the media filters on the class-map, thus allowing more traffic to reach the monitor.

  Workaround: Leave the configuration as-is, or do not broaden the media filters.

- CSCud24483

  Symptom: Dialling FAC (Feature Access Codes) in the On-Hook state and then going Off-hook causes the phone to dial the last called number (Redial Operation).

  Conditions: This symptom occurs when FAC (Feature Access Codes) Standard or Custom is configured.

  Workaround: There is no workaround.

- CSCud37099

  Symptoms: When SIP KPML digits are being received by SIP-GW, they are not consumed even though it is configured to consume those KPML digits. This does not cause the remote endpoint to hear unwanted DTMF tones.

  Platforms: All platforms supporting SIP-TDM GW functionality, which includes ISR-G2 series and VGxx series routers.

Conditions: Whenever SIP-GW negotiates KPML and receives KPML digits from SIP side.

Workaround: There is no workaround.

- CSCud42595

  Symptom: Hit a ipfrag traceback. Mar 12 20:18:34: IOSXE-3-PLATFORM F0: cpp_cp: QFP:0.0 Thread:116 TS:00000154141676112657 FRAG-3-REASSEMBLY_ERR Reassembly/VFR encountered an error: Failed to restore packet persist state -Traceback=1#414e7dc23f4098796bcf8e5a8b3063ad 804c085b 8051a7ae 80276582 80277b0d 80277b6f 80475481 800976d1 804b07e9 Mar 12 20:18:48: IOSXE-3-PLATFORM F0: cpp_cp: QFP:0.0 Thread:082 TS:00000154156360067524 ATTN-3-SYNC_TIMEOUT msecs since last timeout 154149821, missing packets 43

  Conditions: Thiis symptom is observed when fragments received and fragments reassembly related packets are dropped.

  Workaround: There is no workaround.

- CSCud50029

  Symptom: TX drops seen on LSMPI driver show platform software infrastructure lsmpi driver. The reason for the TX drops (sticky):

  ```
  Bad packet len   : 0     Bad buf len     : 0     Bad ifindex     : 0     No device
  : 0     No skbuff        : 0     Device xmit fail : 663  <<<<< ......
  ```

  Conditions: Counter increase due to large control packets.

  Workaround: There is no workaround.

- CSCud50181

  Symptom: ESP crashes when handling srtp-rtp interworking calls.

  Conditions: srtp-rtp interworking enabled.

  Workaround: There is no workaround.

- CSCud52658

  Symptom: IKEv1 CERTREQ payloads exchanged by initiator and responder both contain all trustpoints and trustpools.

  Enhancement: This enhancement request was for limiting the size of the CERTREQ payload by not sending trustpools. Benefits:

  1. The maximum number of trustpoints that can be sent in a CERTREQ payload are 20. But if the user configures more than 15 trustpoints, IKE would fail because of failure to build the CERTREQ payload (16 trustpoints + inbuilt trustpools > 20).

  2. There was a substantial risk for Non-SUDI-enabled devices when authenticating SUDI-enabled devices. This would occur when the non SUDI device has the Cisco Manufacturing Root CA certificate either built-in or downloaded to the device's trustpool. Unless an IKE profile is used, the non SUDI device sends the Mfg CA cert to its peer in the CERTREQ payload.

     If the peer is a SUDI device it might send the SUDI chain in the CERT payload in response. This would result in the device successfully authenticating the peer certificate even though no other trust was configured.

- CSCud60977

  Symptom: CRL file is not deleted when CS server is unconfigured manually by **no crypto pki server <name>**.

Conditions: CS server should be run before server is unconfigured: **crypto pki server <name> no shut**.

Workaround: Delete CRL file manually.

- CSCud61366

  Symptom: fp20 & fp40 cards crashes if single bit parity error occurs on TCAM device#1.

  Conditions: TCAM (hardware) single bit parity errors are very rare and recoverable. Due to a defect in fault recovery code FP crashes instead of recovering from this hardware error.

  Workaround: There is no workaround. May not run into this problem again after FP is rebooted.

- CSCud65119

  Symptoms: A crash might occur while using GETVPN with fragmented IPv6 traffic.

  Conditions: This symptom occurs when IPv6 IPsec is used. This issue is triggered by fragmented IPv6 packets.

  Workaround: There is no workaround.

- CSCud66669

  Symptom: On a 7200 router, the tunnel establishes fine. Encryption and Decryption happens just fine too. However, after decryption, the packet is not punt to the ivrf in which the tunnel interface resides, leading to a broken IPSec DataPath.

  Conditions: 7200 with VSA - Tunnel (GRE/mGRE) in an iVRF with Tunnel protection configuration where the iVRF should not be equal to fVRF.

  Workaround: Since this issue is not found in 150-1.M9 124-24.T8, downgrading might be an option. Otherwise, there is no known configuration related workaround yet, although software crypto will work just fine.

- CSCud67112

  Symptom: In some cases, NBAR does not classify IPv6 HTTP traffic correctly.

  Conditions: May occur with IPv6 HTTP traffic.

  Workaround: In cases where IPv4 addressing is sufficient, use IPv4 as an alternative.

- CSCud67653

  Symptom: ASR1001 (1RU) builtin 4x1GE spa MIB poll for entSensorStatus returns a value of 3 (nonoperational) when CLI sensor reports no reading. No reading is seen from output of **show hw-module subslot all sensors**.

  Conditions: This bug is specific to 1RU (ASR1001) builtin spa 4X1GE.

  Workaround: Possibly, filter entSensorStatus value within customer NMS application.

- CSCud71253

  Symptom: Outbound traffic does not flow.

  Conditions: This symptom occurs when configuring the IPv4 VRF aware IPSec with crypto maps with **ivrf=ivrf1** and **fvrf=global**.

  Workaround: There is no workaround.

- CSCud71606

  Symptoms: The LSMPI Tracebacks errors are seen while clearing IP routes multiple times.

  Conditions: This symptom is observed under the following conditions:

  – Configuring OSPF

  - More than 1000 OSPF neighbors, which fragments OSPF LSU packets.
  - Run **clear ip ospf process ***. OSPF sends an LSU packet, which triggers the LSMPI Tracebacks error message.

  Workaround: There is no workaround.

- CSCud72816

  Symptom: Reload of standby QFP can (rarely) occur.

  Conditions: This symptom is observed when IOS-XE NAT is configured and is used in HA mode (either intrabox or box-to-box) and a **clear ip nat trans** or NAT configuration is changed while there are translations.

  Workaround: There is no workaround, but this is a very rare condition.

- CSCud75554

  Symptom: Previously, when PLAR call was implemented, you needed to disconnect it in order to pickup a ringing call.

  Enhancement: PLAR call disconnect is now supported.

- CSCud75692

  Symptom: Tunnel QoS is broken.

  Conditions: This symptom is observed when the tunnel target interface is ATM sub-interface.

  Workaround: There is no workaround.

- CSCud81011

  Symptom: Sometimes the **fman_aom_cce** traceback is seen.

  Conditions: This symptom is observed only with certain configurations

  Workaround: There is no workaround.

- CSCud81272

  Symptom: When receiving a huge DNS response, the DNS ALG might stop translating, with the response tranparent to the final client.

  Conditions: When one single huge response consumes all init DNS pool entry (1024) and greater.

  1. Config the NAT.

  2. Send dns query response > 12k (vtcp).

  3. Check messages.

  Workaround: There is no workaround.

- CSCud86039

  Symptom: ASR1K router that is running the NAT with a keyword **oer** in the NAT overload mapping can cause disruption to the NATted sessions when the PfR feature changes the exit link.

  Conditions: ASR1K router that is running the NAT with PfR with a **oer** keyword in the NAT configuration can result in this condition.

  Workaround: There is no workaround.

- CSCud88359

  Symptom: Rx traffic drop on the ESP seen by IN_RECV_UNKNOWN_OCT_ERR counter.

  Conditions: When IP header checksum is "0" or "0xFFFF". This counter can be checked using the following command - show platform hardware qfp ac fea ips data drops clear.

Workaround: There is no workaround.

- CSCud94313

  Symptoms: PKI_INV_SPI messages are seen on the console.

  Conditions: This symptom occurs in a FlexVPN setup where Virtual-template is configured and IPsec drops are seen.

  Workaround: There is no workaround.

- CSCud96075

  Symptom: A router running Cisco IOS Release 15.2(4)M2 will reload with a bus error soon after the DSP reloads when there is a live transcoding session.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(4)M2.

  Workaround: There is no workaround.

- CSCue05844

  Symptom: The Cisco 3925 router running Cisco IOS Release 15.0(2)SG reloads when connecting to a call manager.

  Conditions: This symptom is observed with the Cisco 3925 router running Cisco IOS Release 15.0(2)SG.

  Workaround: Remove SNMP.

- CSCue06116

  Symptom: VG350 gateway crashes when the configuration file is downloaded from CUCM. This occurs when the VG350 has 144 ports configured.

  Conditions: The VG350 supports a maximum of 144 FXS ports. Configure MGCP control and download configuration from CUCM, gateway crashes.

  Workaround: Use the no ccm-manager config command to stop the configuration download from CUCM.

- CSCue11507

  Symptom: Transfer call not working via SIP-SIP call in cube IOS 15.3(1).

  Conditions: IOS Version:15.3(1) T Router:3945e

  Workaround: There is no workaround.

- CSCue17800

  Symptom: 6RD and MPLSoGRE tunnel perf drop in x39 throttle more than 5% compared to 3.8 throttle

  Conditions: Perform 6RD and MPLSoGRE tunnel decapsulation.

  Workaround: There is no workaround.

- CSCue20394

  Symptom: Retransmitted SIP request message is calculated for related SIP method counter, however, the counter for other request counter also gets incremented.

  Conditions: This symptom is observed during an ongoing transmission.

  Workaround: There is no workaround.

- CSCue22084

  Symptom: The Create Session Response message is dropped.

Conditions: This symptom is observed when the TEID in Create Session Response message is 0.

Workaround: There is no workaround.

- CSCue22731

  Symptom: WCCP service cannot be enabled.

  Conditions: Two services are configured in same interface, and then one service is deleted while the other is inactive. Then the inactive service cannot be enabled any more.

  Workaround: Do not remove a service from the interface when another service is inactive.

- CSCue22764

  Symptom: **ip wccp check acl outbound** doesn't work on Ultra/Overlord.

  Conditions: Ultra/Overlord platform

  Workaround: There is no workaround.

- CSCue25321

  Symptom: BFD flaps continuously upon ESP switchover.

  Conditions: This symptom is seen upon ESP switchover.

  Workaround: There is no workaround.

- CSCue32352

  Symptom: Non-hdlc traffic (Non standard but customer defined traffic) coming through HDLC interface got dropped by ASR1K.

  Conditions: Normal L2TPv3 configuration.

  Workaround: There is no workaround.

- CSCue33171

  Symptom: The command **show platform software memory chunk qfp-control-process qfp active** shows that there are memory leaks from "CPP STILE Server CTX Chunk". There are three cases of this memory leak: Case 1: when NBAR is active there is a leak of 40 bytes every 10 seconds. Case 2: when NBAR is active there is a leak of 60 bytes every 10 seconds. Case 3: when NBAR is not active there is a leak of 20 bytes every 10 seconds.

  Conditions: Case 1 is observed when the router is running an image with a version prior to 15.3(1)S. Cases 2 and 3 are observed when the router is running version 15.3(1)S or later.

  Workaround: There is no workaround.

- CSCue34694

  Symptom: 2921 Router crashed after receiving 486 Busy.

  Conditions: Observed when handling 486 Busy response.

  Workaround: There is no workaround.

- CSCue39090

  Symptom: A very small FM memory leak is observed.

  Conditions: When attach, detach, or modify a classification policy, a small leak exists.

  Workaround: There is no workaround.

- CSCue39206

  Symptom: ES Crashes after second 401 Challenge.

Conditions: This symptom occurs when second 401 is received after SDP offer/answer with 183/PRACK is complete. This is a rare scenario.

Workaround: There is no workaround.

- CSCue44303

  Symptom: Tracebacks or ESP reload is seen with INFRA-3-INVALID_GPM_ACCESS error msg on standby.

  Conditions: This symptom is seen under low memory conditions.

  Workaround: There is no workaround.

- CSCue46537

  Symptom: Whenever we clear the counters using **clear counters** only the interface counters are getting cleared. Controllers counters never get cleared unless the router is rebooted. In this case, controller is SPA-2XT3/E3.

  Conditions: This symtom is observed only on ASR1K.

  Workaround: Reboot the router.

- CSCue46664

  Symptom: Packet drop may be observed during IP security (IPSec) rekey, in high scaling deployment.

  Conditions: This symptom is observed on a Cisco ASR1000 series router when functions as an IP Security (IPSec) termination and aggregation.

  Workaround: there is no workaround.

- CSCue46852

  Symptom: Local and remote UDP ports are not set correctly in the inbound IPSec Security Association (SA).

  Conditions: This symptom is observed on a Cisco ASR1000 series router when functions as an IP Security (IPSec) termination and aggregation router, and when Tunnel-protection (TP) or Virtual Tunnel Interface (VTI) is deployed, and when IPSec sessions are established behind the Network Address Translation (NAT).

  Workaround: There is no workaround.

- CSCue47484

  Symptom: BFD neighbour is not up.

  Conditions: This symptom is observed after ISSU upgrade of active RP.

  Workaround: There is no workaround.

- CSCue47940

  Symptom: **ip mtu** value `1390` configured in running-configuration and startup-configuration. But after a reboot, its value was changed to `1438`.

  Conditions: After a reboot.

  Workaround: There is no workaround.

- CSCue51792

  Symptom: ASR 1002-X is causing VPN_HW-1-PACKET_ERROR on its IPSEC peer.

Conditions: This was observed only for ASR1002-X for crypto map based tunnels, with tunnel keepalive enabled on the peer, and esp-3des as encryption mechanism. Only the GRE returning keepalive seems to be affected; the rest of the traffic is unaffected.

Workaround: Use one of the following:

- Disable gre keepalives on the peer.
- Use AES instead of DES as encryption mechanism.
- Move towards tunnel-protection-based design instead of cryptomap, and use IPSEC/IKE keepalives instead of GRE keepalives.

- CSCue51886

  Symptoms: The SBC CUBE device rejects call connections.

  Conditions: This symptom is observed when the Chunkmanager holds a lot of memory and calls do not get processed.

  Workaround: Reloading the box helps to make the box stable.

- CSCue51967

  Symptom: An ASR1K or ISR 4400 router may experience service interruptions and may encounter a QFP microcode software exception. The log will indicate that the router processor has crashed and restarted.

  Conditions: The router is performing DMVPN tunneling or is operating as an AppNav controller while collecting data for AVC.

- CSCue52065

  Symptom: With WCCP configured, when you replace the configuration, you get get continuous traceback on the console at **fman_wccp_aom_batch_begin**.

  Condition: Race condition when WCCP interface / WCCP ACL are configured in several miliseconds.

  Workaround: There is no workaround.

- CSCue59759

  Symptom: When an AVC policy is assigned to a DMVPN tunnel interface, the packet count in AVC records may be incorrect.

  Conditions: Can occur when an AVC policy is assigned to a DMVPN tunnel interface.

  Workaround: No known workaround.

- CSCue59891

  Symptom: When Priority-queue 100% is configured on class-default, packets are not going on High ESI.

  Conditions: When Priority-queue 100% is configured on class-default, packets are not going on High ESI.

  Workaround: There is no workaround.

- CSCue61481

  Symptom: After hard OIR, **show inventory** does not show inventory info.

  Conditions: hard OIR

  Workaround: There is no workaround.

- CSCue63181

Symptom: The Delete PDP Context Response message is dropped.

Conditions: This symptom is observed when Delete PDP Context Request is rejected.

Workaround: There is no workaround.

- CSCue68258

  Symptom: In IOS-XE releases 15.3(1)S2 and 15.3(2)S, upon performing an RP switchover, the following message might be displayed on the console of the newly active RP:

  ```
  %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F1: fman_fp_image:
  Modify not supported for FLOW-DEF:<> download to CPP failed
  ```

  Furthermore, this might cause some of the features on the newly active RP to have stale objects, which can be observed by issuing the following command:

  show platform software object-manager FP active statistics

  Conditions: The above message appears when Flexible NetFlow was configured on the previously active RP.

  Workaround: The only workaround available is to not do an RP switchover. However, if you do go ahead with an RP switchover and end up in the inconsistent state noted above, you can perform one of the following actions to bring the router back to a consistent state on the newly active RP.

  - Save the running configuration to NVRAM and reload the new RP.
  - Alternatively, if the system has dual FPs, then perform two FP switchovers successively:
    1. Switch over from active FP to standby FP using **redundancy force-switchover FP**.
    2. Switch back from standby to active using the same command.

- CSCue69075

  Symptom: BDI interface stops forwarding the traffic.

  Conditions: This symptom is observed when there is a loop in data path.

  Workaround: Recreate the BDI interface.

- CSCue71410

  Symptom: Console corruption is seen sometimes when the punt keepalive packet drop happens during bootup of the router.

  Conditions: This symptom is observed when punt keepalive packet is dropped and other console activity is going on at the same time.

  Workaround: Punt keepalive messages can be disabled in the config, but it is not a recommended setting as it can mask punt failures.

- CSCue72258

  Symptom: A Cisco ASR1000 series router cannot forward specific size of packets via L2TPv3 tunnel.

  Conditions: The problem occurs only when the ping size is 1501-1503.

  Workaround: There is no workaround.

- CSCue76134

  Symptom: With NAT dynamic route-map configuration and HA, lower pool allocation is displayed on the standby.

Conditions: With NAT dynamic route-map configuration and HA, you sometimes see a lower pool allocation on the standby compared to the active. This could be caused by DNS traffic going through the boxes.

Workaround: Perform the following:

1. **clear ip nat trans ***
2. Turn off DNS ALG on the both active and standby boxes, if possible.
3. **no ip nat service dns tcp no ip nat service dns udp**

- CSCue82511

  Symptom: The traffic-classes keeps switching between the Border Routers and PfR fails to converge.

  Conditions: The issue is seen when PfR Border Routers are deployed over different platforms.

  Workaround: The workaround is to use the same platform for all the PfR Border Routers.

- CSCue83147

  Symptoms: WCCP does not work properly with IPSEC/PBR/ZBF/NAT together or vice versa.

  Conditions: Configured IPSEC/WCCP/PBR/ZBF/NAT in the same interface.

  Further Problem Description: This defect is to track the rework of the WCCP feature so that it can work together with IPSEC/PBR/ZBF/NAT.

  Workaround: There is no workaround.

- CSCue87883

  Symptom: NAT might not release some of its ALG-related memory.

  Conditions: NAT having a large memory footprint after several hours of traffic failed FTP64 ALG traffic.

  Workaround: Reload and turn off FTP64 ALG: **no nat64 service ftp**.

- CSCue88591

  Symptom: DSP error message printed on console, and crash takes place.

  Conditions: DSP firmware (version:33.1.00) sends corrupted DSP error message to RP IOS, which leads to crash:

  ```
  %SPA_DSPRM-3-DSPALARM: Received alarm indication from dsp (1/0/9).
  %SPA_DSPRM-3-DSPALARMINFO: 0008 0000 0080 0000 0000 0001 7F3B FEDF
  %SPA_DSPRM-3-DSPALARMINFO: ;????
  %DSP-3-DSP_ALARM: SIP1/0: DSP device 2 is not responding. Trying to recover DSP device by reloading
  ```

  Workaround: Downgrade to XE36, which runs firmware v. 31.1.0

- CSCue89006

  Symptom: SIP ALG creates PAT translation before portlist.

  Conditions: This is a SIP ALG cooperation for consistency with NAT modification on defect CSCuc85157 for PAT. This resolves a problem since v. XE37.

  Workaround: There is no workaround.

- CSCue90034

  Symptom: The router cannot be booted up.

  Conditions: onefw configuration.

Workaround: Remove the onefw configuration.

- CSCue94610

  Symptoms: DSP crash with the following console error:

  ```
  %SPA_DSPRM-3-DSPALARMINFO: Checksum Failure:80000000,0000000e,d0156a80,d0156000
  *Mar 14 17:56:05.851:
  %SPA_DSPRM-3-DSPALARM: Received alarm indication from dsp (1/3/6).
  %SPA_DSPRM-3-DSPALARMINFO: 0042 0000 0080 0000 0000 0000 4368 6563 6B73 756D 2046
  6169 6C75 7265 3A38 3030 3030 3030 302C 3030 3030 3030 3065 2C64 3031 3536 6138
  302C 6430 3135 3630 3030 0000 0000 0000 0000 0000
  ```

  Conditions: Error occurs during an RP switchover process. The standby RP presents DSPs failing to come up.

  Workaround: This command may clear up the DSPs:

  ```
  Router# hw-module subslot x/y reload
  ```

- CSCue97118

  Symptom: Cube crashes when codenomicon test is run. This is basically a stress test that checks the boundary condition for a large From header sent in invite.

  Conditions: Very large From header in incoming SIP invite.

  Workaround: Fix provided in stack, to handle these error scenarios properly.

- CSCue97338

  Symptom: Update PDP context request is dropped.

  Conditions: TEID is 0, IMSI is existing.

  Workaround: There is no workaround.

- CSCue97986

  Symptom: Hung call at SIP, CCAPI, VOIP RTP components (but cleared in the Dataplane of ASR1k platform).

  Conditions: Video call set up as audio call. Call then gets transferred with REFER but caller hangs up the call before the call gets transferred. This is an intermittent problem.

  Workaround: There is no workaround.

- CSCuf01088

  Symptom: Memory leaks are observed in ASR with CVP call flows.

  Conditions: Under load condition, memory leaks are seen in XE3.8.

  Workaround: There is no workaround.

- CSCuf02990

  Symptom: Users might experience high CPU utilization during AVC bringup. Bring-up process does not converge correctly and introduces an unexplained high CPU utilization with traffic.

  Conditions: AVC bringup after CPU regulation mechanism turns off service.

  Workaround: There is no workaround.

- CSCuf04906

  Symptom: ASR crashes when running VZ Inst image with VZ call flows.

  Conditions: Crashes under load conditions.

  Workaround: Fix given. While confId is valid, do a hash entry search.

- CSCuf15260

  Symptom: ASR box crashes while sending Notify with KPML Digit.

  Conditions: ASR DTMF type is changing to SIP-KPML mid-call.

  Workaround: Do not change DTMF type mid-call.

- CSCuf25232

  Symptom: Crashes are seen in CUCM code, which is applicable for IOS stack also.

  Conditions: Not known. See also CSCtz08251 and CSCua92010.

  Workaround: There is no workaround.

- CSCuf29121

  Symptom: System crash.

  Conditions: On ASR1002 system with ipsec is configured on both ingress and egress GRE tunnel interface and configure NAT64 feature with FTP stateful traffic, the system crashes.

  Workaround: configure "no nat64 service ftp" to disable FTP64 ALG, system does not crash with FTP stateful traffic.

- CSCuf36495

  Symptom: This defect is a placeholder for adding MPLS awareness to FNF for Software Release 15.3(01)S2. The added code is only for QFP processor code and not for IOS support.

  Conditions: FNF - Port MPLS aware ucode changes to XE38 throttle.

  Workaround: There is no workaround.

- CSCuf51881

  Symptom: Memory is holding up on CUBE if the KPML Subscription expiration timer is too big and no unsubscribe is received.

  Conditions: This is seen for KPML subscription duration too high under load, with no unsubscribe received.

  Workaround: There is no workaround.

- CSCuf56490

  Symptom: This defect is a placeholder for adding MPLS awareness to FNF for Software Release 15.3(1)S1.

  Conditions: FNF - Port MPLS aware PAL changes to XE38 throttle

  Workaround: There is no workaround.

- CSCuf56693

  Symptoms: Traceback might appear when configuring NBAR custom protocol on Border Router.

  Conditions: This symptom is observed when PfR is "updating" or "deleting" Traffic-Classes during NBAR custom protocol configuration.

  Workaround: Before configuring NBAR custom protocol, shut the PfR-Master.

- CSCuf60585

  Symptom: cpp_cp_svr crash at cpp_qm_event_insert_aggr_node.

  Conditions: While bringinup 4K PPPoA sessions with QOS policy attached in ATM subinterfaces.

  Workaround: There is no workaround.

- CSCug01256

Symptom: QMovestuck is observed when you attempt to change the policy map with traffic ON.

Conditions: This is seen when changes are made in policy-map with traffic ON.

Workaround: Reload the router to bring it back to normal state.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8.1S

This section describes the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8.1S. It contains the following topics:

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.8.1S

This section documents the unexpected behavior that might be seen in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8.1S.

- CSCtv93326

  Symptom: Inconsistency between IOS CLI and platform state with regard to flow record configuration on the router. Reporting of Mediatrace statistics may fail, with the following error reported on the Mediatrace Initiator device: `Metrics Collection Status: Fail (19, No statistic data available for reporting)`

  Conditions: This is a Flowdef modify event as a result of event consolidation. It can occur in the following scenario: 1. Detach the flowdef associated with a monitor. 2. Change the flowdef (add / delete fields). 3. Re-attach the flowdef to the monitor. For the Mediatrace symptom, the problem can occur when a route change occurs for the traffic being monitored.

  Workaround: There is no workaround.

- CSCua68587

  Symptom: cvCallVolConnActiveConnection.sip MIB count does not match what is seen on the CLI.

  Conditions: This symptom is observed with the Cisco ASR 1006 running Cisco IOS XE Release 3.6.0S or Cisco IOS Release 15.2(2)S with the asr1000rp2-adventerprisek9.03.06.00.S.152-2.S image.

  Workaround: There is no workaround.

- CSCub17971

  Symptom: No re-registration after switching from hardware to software crypto engine.

  Conditions: As per the plan, registration should happen after switching from hardware to software.

  Workaround: There is no workaround.

- CSCub19185

  Symptoms: Path confirmation fails for a SIP-SIP call with IPV6 enabled.

  Conditions: This symptom occurs when UUTs are running Cisco IOS Release 15.2(2)T1.5.

Workaround: There is no workaround.

- CSCub53856

  Symptom: On ASR1K and related platforms, when configuring a Flow NetFlow (FNF) Performance Monitor with a record that has a large number of fields (typically 30 or more), the following traceback may be observed at the time that the Service Policy is bound to the interface:

  ```
  %FNF-3-FNF_FIELD_LIST_TOO_LARGE: Field_list too large, max 32
  ```

  Conditions: Configuring a Performance Monitor, typically with more than 30 fields, and binding it to an interface via a Service Policy.

  Workaround: Reduce the number of fields. Using fewer than 30 should work, although it does depend on the exact fields in the record.

- CSCuc12685

  Symptoms: A router has an unexpected reload in SIP code.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M4.

- Workaround: There is no workaround.

  CSCuc27517

  Symptom: The permanent license disappears after an IOS upgrade or downgrade.

  Conditions: ASR1001 IOS upgrade from 03.05.02 or older to 03.06.00 or later IOS downgrade from 03.06.00 or later to 03.05.02 or older.

  Workaround: Install permanent license again.

- CSCuc42518

  Symptom: Cisco IOS Unified Border Element (CUBE) contains a vulnerability that could allow a remote attacker to cause a limited Denial of Service (DoS). Cisco IOS CUBE may be vulnerable to a limited Denial of Service (DoS) from the interface input queue wedge condition, while trying to process certain RTCP packets during media negotiation using SIP.

  Conditions: Cisco IOS CUBE may experience an input queue wedge condition on an interface configured for media negotiation using SIP when certain sequence of RTCP packets is processed. All the calls on the affected interface would be dropped.

  Workaround: Increase the interface input queue size. Disable Video if not necessary.

- CSCuc58527

  Symptom: Mac flush does not happen properly with events like Interface shut/noshut or BD shut/noshut.

  Conditions: This symptom is observed when the mst root priority on R-l2gp config is changed to make the other PE to become root.

  Workaround: Use the old CLI format.

- CSCuc73993

  Symptom: High packets per second (PPS) in single flow traffic may reduce overall system performance by 90%.

  Conditions: Occurs when there is a very high PPS value in single flow traffic, and when NBAR is enabled.

  Workaround: There is no workaround.

- CSCuc76298

Symptom: In the ASR B2B HA setup, a new active router crashes at ccsip_send_ood_options_ping immediately after a switchover with OOD OPTIONS enabled.

Conditions: This crash is seen when a standby router has OOD OPTIONS enabled either because it is present in the startup config or enabled after the bootup. When you disable the OOD OPTIONS, the switchover happens.

Workaround: Reload standby router once after OOD OPTIONS config changes from enabled to disabled.

- CSCuc93739

  Symptom: Phase 2 for EzVPN client with split network and VTI does not come up if IPSEC SA goes down.

  Conditions: The root cause of the issue is that IPsec SA is not being triggered after IPsec SA is down due to no traffic. This causes IPsec SA to not come UP in spite of the traffic, leading to packet drops in client network. The same problem is not seen with 150-1.M7. This behavior is seen post-PAL where virtual-interface creates a rule set where traffic cannot trigger IPsec SA again once IPsec SA is deleted.

  Workaround: 1. Configure ?ip sla? on EZVPN client for split networks, so IPsec SA will not go down. 2. Remove ?virtual-interface? from EZVPN client profile if that is not needed. The problem is not seen in 152-4.M1 without virtual-interface.

- CSCud14945

  Symptom: IPv4 IP Security (IPSec) tunnel bring up time is longer in the dynamic crypto-map deployment.

  Conditions: This symptom is observed on a Cisco ASR1000 series router that functions as an IPSec termination and aggregation router.

  Workaround: There is no workaround.

- CSCud19536

  Symptom: In AVC for IOS XE 3.8, a short downtime is experienced after modifying the AVC configuration.

  Conditions: The symptom is observed when removing the media filters on the class-map, thus allowing more traffic to reach the monitor.

  Workaround: Leave the configuration as-is, or do not broaden the media filters.

- CSCud50029

  Symptom: TX drops seen on LSMPI driver show platform software infrastructure lsmpi driver. The reason for the TX drops (sticky):

  ```
  Bad packet len   : 0    Bad buf len     : 0    Bad ifindex     : 0    No device
  : 0     No skbuff        : 0     Device xmit fail : 663  <<<<< ......
  ```

  Conditions: Counter increase due to large control packets.

  Workaround: There is no workaround.

- CSCud64870

  Symptom: DMVPN hub ASR1004 may crash after the fetching CRL from MS CRL server.

  Conditions: The crash occurs when there are 5 CDPs for the hub router to fetch the CRL. Since there are multiple CDPs, the hub router fetches the CRL in a parallel way, which leads to a crash under a timing issue.

  Workaround: Setting up one CDP instead of multiple CDPs will avoid the timing condition that leads to the crash.

- CSCud66669

  Symptom: On a 7200 router, the tunnel establishes fine. Encryption and Decryption happens just fine too. However, after decryption, the packet is not punt to the ivrf in which the tunnel interface resides, leading to a broken IPSec DataPath.

  Conditions: 7200 with VSA - Tunnel (GRE/mGRE) in an iVRF with Tunnel protection configuration where the iVRF should not be equal to fVRF.

  Workaround: Since this issue is not found in 150-1.M9 124-24.T8, downgrading might be an option. Otherwise, there is no known configuration related workaround yet, although software crypto will work just fine.

- CSCue19713

  Symptom: ASR1013 route processor (RP) reloads due to a watchdog reset.

  Conditions: This issue is seen with a power supply which reports fan failure/recovery events continuously.

  Workaround: Replace the power supply.

- CSCue21381

  Symptom: CUBE ASR 1K crashes during the VOIP FPI process.

  Conditions: As of now, the specific call flow leading to this crash is not narrowed down, but based on the code analysis and trace back, it is suspected to happen during the call transfer flow.

  Workaround: There is no workaround.

- CSCue25321

  Symptom: BFD flaps continuously upon ESP switchover.

  Conditions: This symptom is seen upon ESP switchover.

  Workaround: There is no workaround.

- CSCue27533

  Symptom: Multi-VRF Selection with PBR and return traffic is dropped.

  Conditions: ASR1002-F/03.07.01.S.

  Workaround: Static route in GRT.

- CSCue39206

  Symptom: ES Crashes after second 401 Challenge.

  Conditions: This symptom occurs when second 401 is received after SDP offer/answer with 183/PRACK is complete. This is a rare scenario.

  Workaround: There is no workaround.

- CSCue42193

  Symptom: ASR1k with GetVPN and a large number of ACLs may see tracebacks and fman_fp crashes on ESP.

  Conditions: GetVPN setup and ACLs configured may see these symptoms if the ACL is being modified.

  Workaround: Do not modify the ACL.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.8.1S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8.1S.

- CSCtx59316

  Symptom: A packet punt to RP due to incomplete adjacency gets processed by CoPP. This makes the CoPP complex, as these punted packets are not directed to the system and requires the CoPP to be opened up.

  Conditions: This symptom is seen with 3.5.2S and similar releases and by current design.

  Workaround: Change the CoPP to allow punted packets.

- CSCua56879

  Symptom: XE37 and XE38 images are running with PTP code.

  Conditions: XE37 and XE38 are running with PTP code. This feature is not supported in these releases.

  Workaround: There is no workaround.

- CSCua90697

  Symptom: Traffic-class cannot be learned with delay as learning type reports is incorrect in a number of TCs.

  Conditions: Configurate delay as learning type.

  Workaround: There is no workaround.

- CSCub50350

  Symptom: Remote loopback messages under `show interface` and `show controller` output are not set correctly.

  Conditions: Remote loopback configuration.

  Workaround: There is no workaround.

- CSCub50695

  Symptom: Netflow data may be fragmented when using IPv6 exporter.

  Conditions: 1. IPv6 exporter is used. 2. A large amount of data are exported at once.

  Workaround: There is no workaround.

- CSCub57913

  Symptom: The memory of ESP is exhausted.

  Conditions: This symptom is observed when you use the **show platform hardware qfp active feature pfr** command a number of times.

  Workaround: There is no workaround.

- CSCub74272

  Symptom: Intermittently during Phase II rekey, after new SPIs are negotiated and inserted into SPD, old SPIs are removed and then the VTI tunnel line protocol goes down.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T, with VTI over GRE.

  Workaround: There is no workaround.

- CSCub78299

  Symptom: Ping fails from host1 (192.168.1.2) to host2 (192.168.4.2).

  Conditions: This symptom is observed when Suite-B is configured on IPsec sa.

  Workaround: There is no workaround.

- CSCub83071

  Symptom: Traceback is observed during RP switchover with mediatrace configuration, since SSO is not supported by mediatrace.

  Conditions: Configure mediatrace. Perform RP switchover twice.

  Workaround: Remove mediatrace configuration before running RP-switchover. Add mediatrace configuration on new active RP. Or, If traceback occured, remove mediatrace configuration and reapply it.

- CSCub86791

  Symptom: The maximum active memory for NBAR flows will exceed the maximum allowed memory.

  Condition: This symptom is observed on the 1RU platform with XE3.8 installed. The maximum flows are set to 750000, but the traffic contains flows higher than 750000.

  Workaround: There is no workaround.

- CSCub89144

  Symptom: The VTI tunnel is always in up/up state.

  Conditions: This symptom is observed when HSRP failover is configured on the HSRP standby router only. This issue was first seen on the Cisco ASR router, but it is platform-independent and is seen on the latest Cisco IOS Release 15M&T and later releases as well.

  Workaround: Use GRE or routing protocols for redundancy.

- CSCub98177

  Symptom: ASR1K as LAC running IOS XE RLS3.5.2 may disconnect PPP session by TermReq without visible reason, each time in `show pppoe stat` incrementing `SSM DISCONNECT`.

  Conditions: This symptom is observed in SSO mode, with RP switchover.

  Workaround: There is no workaround.

- CSCuc00658

  Symptom: Unable to ping direct connected peer ip address.

  Conditions: 1. Configure IP reassembly on sub interface. 2. Configure IPv6 reassembly on the same sub interface. 3. No sub interface.

  Workaround: There is no workaround.

- CSCuc05174

  Symptom: ESP Crashes.

  Conditions: Configuration results in exhaustion of CPP external memory.

  Workaround: Ensure that the scale does not exceed supported configurations.

- CSCuc08061

  Symptom: IPv6 DMVPN spoke fails to rebuild tunnels with hubs.

Conditions: This symptom occurs when the tunnel interface on the spoke is removed and reapplied again.

Workaround: Reboot the spoke.

- CSCuc25529

  Symptom: Static routes created by RRI are created with the wrong mask for subnet ACLS.

  Conditions: This symptom is observed on an ASR1k and 7200 platforms running IOS 15.2(4)S and 15.1(4)M.

  Workaround: Configure a static route to the remote network manually.

- CSCuc30500

  Symptom: The features NBAR, FNF (AVC), Seawolf (FME), and Lhotse (AppNav) may appear to be activate even when they are down.

  Conditions: This symptom is observed when CFT infra is not initialized on these features.

  Workaround: There is no workaround.

- CSCuc32543

  Symptom: Changes in the configured ppp multilink fragment size or fragment delay are not pushed down to the data path for Broadband MLPPP sessions. This issue does not apply to MLPPP over Serial connections.

  Conditions: If ppp multilink fragmentation is enabled on a Broadband MLPPP bundle before the bundle is established and the user later attempts to modify the fragment size or fragment delay, the resulting fragment size changes are not pushed down to the data path (i.e. the original fragment size configuration is retained). The IOS **show ppp multilink** command indicates that the new fragment size was applied but in fact the new fragment size may not yet be active.

  Workaround: After changing the fragment size or fragment delay configuration, restart the Multilink PPP session. This can be accomplished via the **clear ppp interface *<Bundle-Virtual-Access-intf-name>*** command.

- CSCuc36469

  Symptom: A crash is observed when you remove the `crypto call admission limit ike in-negotiation-sa <value>` configuration and clear crypto sessions, which triggers a connection from all the clients burdening the server and forcing it to crash within seconds.

  Conditions: This symptom is observed only when 150 connections simultaneously try to establish connection with the Head-end Ezvpn server.

  Workaround: Ensure you always configure `crypto call admission limit ike in-negotiation-sa 20` when scaling to 150 tunnels.

- CSCuc39469

  Symptom: Unable to monitor the newly inserted 2nd Power supply in ASR1001.

  Conditions: Insert the 2nd Power Supply to the up and running ASR1001.

  Workaround: Ensure that all power supplies are inserted before booting up the ASR1001.

- CSCuc41243

  Symptom: PfR border router might get reloaded when PfR session flap is under session condition.

  Conditions: PfR BR session flap is under session condition. This condition cannot be reproduced in the lab.

  Workaround: There is no workaround.

- CSCuc44071

  Symptom: GRE keepalives go out unencrypted if the Tunnel interface is in **up / protocol down** state.

  Conditions: ASR1k platform (reproduced on 3.4S through 3.7S) - GRE/IPsec using tunnel protection - keepalives configured on GRE/IPsec tunnel - Tunnel interface in protocol down state because of previously missed GRE keepalives - PIM configured on Tunnel interface - **ip multicast-routing distributed** configured globally.

  Workaround: Disable **ip multicast-routing distributed** (possible performance impact) or remove PIM configuration from Tunnel interface. The GRE keepalives will be encrypted as long as there is no CEF adjacency on the Tunnel interface when in protocol down state (i.e. no output from **show adjacency tunnel <number> detail** command).

- CSCuc59991

  Symptom: The traceback may appear in applying or removing Cisco Application Visibility and Control configuration.

  Conditions: The traceback may appear in a very rare condition of massive applying or removing Cisco Application Visibility and Control configuration sequence.

  Workaround: In case of traceback, remove the configuration and reapply it again.

- CSCuc62212

  Symptom: **sh pla so ob fp active pending-ack-update** output hw dirty-bit has error.

  Conditions: There are no specific conditions.

  Workaround: There is no workaround.

- CSCuc65424

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

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

  Workaround: Turn off the IDB reuse option.

- CSCuc67116

  Symptom: IPSec SA reset when sequence number rolls over back to 0 with anti-reply disable.

  Conditions: OUT_OCT_DETECT_SEQ_OVEFLOW counter increase.

  Workaround: There is no workaround.

- CSCuc70310

  Symptom: RRI routes are not installed in DMAP. **reverse-route** is a configuration in the DMAP. This prevents packets from being routed through the intended interface, and hence packet loss occurs.

  Conditions: This symptom is observed when a simple reverse-route is configured in DMAP without any gateway options.

  Workaround: There is no workaround.

- CSCuc70578

  Symptom: While clearing the counters, the following error message is seen:

  ```
  %IOSXE-3-PLATFORM: R0/0: kernel:
  /scratch/mcpre/BLD-BLD_V153_1_S_XE38_THROTTLE_LATEST_20121015_080026/os/linux/drive
  rs/binos/i2c/psmcu/psmcu_main.c:read_from_psmcu (line 185): i2c_smbus_read_byte()
  ```

```
returned -110  Other potential errors: %IOSXE-3-PLATFORM: R0/0: kernel:
/auto/mcpbuilds13/release/03.08.00.S/BLD-03.08.00.S/os/linux/drivers/binos/i2c/psmc
u/psmcu_main.c:read_from_psmcu (line 175): MCU set pointer command failed, -5.
```

Conditions: Error message seen while clearing the counters.

Workaround: There is no workaround.

- CSCuc72643

  Symptom: Periodic memory leak occurs.

  Conditions: This symptom is observed periodically.

  Workaround: There is no workaround.

- CSCuc73993

  Symptom: High PPS of single flow traffic may reduce the overall system performance by 90%.

  Conditions: This symptom is observed when there is very large PPS of single flow traffic, and when NBAR is enabled.

  Workaround: There is no workaround.

- CSCuc74857

  Symptom: NAT address pool exhaustion with high DNS traffic.

  Conditions: Payload addresses in DNS PTR record natted without active NAT bindings. RFC 2694 suggests that DNS PTR queries should not be translated if no active bindings are found in the NAT translation table. Per current implementation, new NAT dynamic bindings are created when processing DNS PTR queries, eventually contributing to NAT address pool exhaustion.

  Workaround: 1. Add deny ACL to avoid NAT translation of unknown payload addresses in the DNS PTR query. 2. Turn off dns alg service if possible.

- CSCuc76130

  Symptom: IPsec SAs are not getting deleted even after removing ACL.

  Conditions: This symptom occurs when you use the IPsec feature with Cisco IOS Release 15.3(0.18)T0.1.

  Workaround: There is no workaround.

- CSCuc76566

  Symptom: The **show platform hardware qfp active feature ess session** command is supposed to display a list of features enabled on each session. The status of the FFR feature is not displayed.

  Conditions: It affects debuggability of mobility IP sessions on iWAG.

  Workaround: There is no workaround.

- CSCuc77704

  Symptom: The GETVPN/GDOI Secondary Cooperative Key Server (COOP-KS) does not download the policy (that is, when the show crypto gdoi ks policy command is issued on the Secondary COOP-KS and the command output shows that no policy is downloaded) and Group Members (GMs) registering to the Secondary COOP-KS fail to register without any warning/error message.

  Conditions: This symptom is observed when the GETVPN/GDOI group (with COOP configured) has an IPsec profile configured with one of the following transforms in its transform-set: - esp-sha256-hmac - esp-sha384-hmac - esp-sha512-hmac.

  Workaround: Use esp-sha-hmac as the authentication transform instead.

- CSCuc78499

  Symptom: GTPv1 memory chunk leak.

  Conditions: GTP AIC is configured.

  Workaround: There is no workaround.

- CSCuc78702

  Symptom: `%NAT: VRF ID 2385 does not exist` seen in the output of **show run vrf** .

  Conditions: If a VRF is defined without configuring an address-family, then this message may be displayed when the user issues a **show running vrf** command.

  Workaround: The show command output is still valid. This has no impact on the functionality.

- CSCuc79208

  Symptom: Error `%Port <>` is being used by system. When configuring static nat with the same ports for different IP addresses as shown below, you may see following error message: `"%Port 1720 is being used by system" : ip nat inside source list IP_PBX_MP_NAT_ACL_PUB interface Loopback12 overload ip nat inside source list IP_PBX_MP_NAT_ACL_SUB interface Loopback13 overload ip nat inside source static tcp 161.92.7.42 1720 interface Loopback12 1720 ip nat inside source static tcp 161.92.7.43 1720 interface Loopback13 1720.` This issue occurs when you have NAT with overload statements configured before you configure static NAT for ports.

  Conditions: This symptom is observed when NAT with overload statements are configured first.

  Workaround: Remove all NAT statements and configure static NAT before NAT overload. (You may see the failure again at reload time since the commands are nvgenned with the overload command first.)

- CSCuc80725

  Symptom: **vfr subblock** remains without displaying the **ip virual-reassembly** command.

  Conditions: This symptom is observed when you enable NAT and **no vfr**, and re-enable **vfr**.

  Workaround: Enable **no vfr** manually.

- CSCuc81645

  Symptom: Execute the show command and cpp crashes on overlord.

  Conditions: None.

  Workaround: There is no workaround.

- CSCuc81662

  Symptom: ISR4451 Router doesn't boot properly. The slot F0 stays in init state.

  Conditions: This symptom is observed just after a power cycle. This condition is rare and is seen once every few hundred power cycles.

  Workaround: Power cycle the router, a soft reload will not clear this issue.

- CSCuc85002

  Symptom: Unexpected logs printed in the console during configuration.

  ```
  *Oct 17 06:54:50.711: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F1: fman_fp_image:  PORTLIST: (tcp/50.1.1.1 port 4096 - 5119) download to CPP failed  *Oct 17 06:54:50.534: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image:  PORTLIST: (tcp/50.1.1.1 port 4096 - 5119) download to CPP failed.
  ```

Conditions: This symptom is seen when the configuration includes dynamic PAT (port address translation) with interface overload.

Workaround: There is no workaround.

- CSCuc85807

  Symptom: In cases where MMON is activated on non-video UDP, traffic jitter values of certain flows may have incorrect jitter values.

  Conditions: Non video and/or UDP traffic is being injected to the MMON engine. It may also happen to video traffic before it is classified as such (first few packets) - this is self corrective. This is unlikely to happen since usually MMON is enabled on specific media flows.

  Workaround: There is no workaround.

- CSCuc87847

  Symptom: QFP crashes.

  Conditions: Packets are replicated and field **in_interface** in **pkt_state** is invalid.

  Workaround: There is no workaround.

- CSCuc88175

  Symptom: When a dynamic cryptomap is used on the Virtual Template interface, SAs do not get created and thus the testscripts fail. This issue occurs because the crypto map configurations are not added to the NVGEN, and there is no security policy applied on the Virtual Template interface.

  Conditions: This symptom is observed only when a dynamic map is used on the Virtual Template interface. However, this issue is not seen when tunnel protection is used on the Virtual Template interface or when a dynamic map is used on the typical physical interface.

  Workaround: Use tunnel protection on the Virtual Template interface.

- CSCuc89646

  Symptom: When TCP SYN packet is sent with no MSS specified, the default value is set to 0, not 536, as on other platforms.

  Conditions: TCP SYN packet is sent with no MSS specified.

  Workaround: There is no workaround.

- CSCuc89800

  Symptom: ESP crashes when it receives a for_us packet with multiple (thousands of) tunnel headers.

  Conditions: This symptom is observed in a scenario where there are three routers, A, B, and C, and there is a tunnel T1 between A and C. In router A, a PBR transmits the packets from B through T1. In router B, a default route points to router A. Router A then transmits a packet through the T1 tunnel, encapsulated with a GRE header. When this packet arrives at router B, due to the flapping of route between B and C, it is not sent to router C. Instead, it is sent to router A because router A is the default route. When the packet arrives at router A, it is transmitted through the T1 tunnel again encapsulated with another GRE header. This cycle continues and the packets are encapsulated with thousands of GRE headers. Finally, when the route between B and C no longer flaps, it arrives at router C, causing it to crash.

  Workaround: Configure an ACL in router C's tunnel T1 interface, and deny the packet if it has an inner header with the same src addr and dst addr with outer the header. But this workaround cannot cover the scenario that has an attack packet encapsulated with multiple different tunnel headers.

- CSCuc92567

  Symptom: SIP may reload during MDR due to ESI reconciliation failure with active ESP.

Conditions: Extremely rare race condition.

Workaround: There is no workaround.

- CSCuc93053

  Symptom: WCCP stops working after adding ZBF. We see a message of WCCP packets being redirected but not leaving ASR.

  Conditions: ASR with netflow anf ZBF enabled under the same interfaces.

  Workaround: Disable netflow on all the interfaces.

- CSCuc93807

  Symptom: Metrics that require AOR are not accounted correctly. (for example: ART metrics, packet/bytes counter and so on.)

  Conditions: 1. Performance policy map is configured with parameter default account-on-resolution property. 2. At least one NBAR filter is presented in one of the class-maps of the policy-map. 3. Packets are matched by the class-map without any monitor.

  Workaround: Add a flow monitor (even without an exporter) to the class-default.

- CSCuc95192

  Symptom: Ucode Crash Seen.

  Conditions: Unconfigure/Configure static NAT in B2BHA setup.

  Workaround: There is no workaround.

- CSCuc97477

  Symptom: This is a new feature for dummy packet support.

  Conditions: None.

  Workaround: There is no workaround.

- CSCuc98107

  Symptom: The performance of urpf with acl gets downgraded.

  Conditions: The downgrading is found on Release 15.3(01)S onwards.

  Workaround: There is no workaround.

- CSCuc97789

  Symptom: The hostname reporting is not supported.

  Conditions: It is observed when the AVC URL tool is configured and the http traffic sends the hostname that are not reported.

  Workaround: There is no workaround.

- CSCud01905

  Symptom: Match not apn is not working.

  Conditions: Basic gtp message flow.

  Workaround: There is no workaround.

- CSCud03863

  Symptom: ESP crashes on CSR.

  Conditions: Crash occurs when sending traffic through a non gig 0 interface.

  Workaround: There is no workaround.

- CSCud04066

  Symptom: CPP CVLA traceback appears.

  Conditions: This may occur during monitor configuration rollback when configuration fails.

  Workaround: There is no workaround.

- CSCud05368

  Symptom: Traffic will be redirected to WCCP client even when it is defined as deny in wccp redirect ACL.

  Conditions: WCCP on ASR1k.

  Workaround: There can be two workarounds: 1. Move the deny entries before the permits when possible (especially for deny ... host ...), but it still may not work in some situations. 2. Use different redirect ACLs for each service, and remove the unnecessary ones for specific services.

- CSCud06852

  Symptom: T1 Controller will not be marked as DOWN when there are alarms after the RP Switchover.

  Conditions: RP Switchover.

  Workaround: SPA Soft OIR.

- CSCud06887

  Symptoms: IPsec Stateful failover is configured between two routers. router 1 is chosen as Active. router 2 is chosen as Standby. router 3 acts as the VPN end peer. A VPN tunnel is created between the VIP of routers 1 and 2 and router 3. SPIs are replicated from Active (router 1) to Standby (router 2). After switchover from Active to Standby (done by reload of Active router 1), router 2 becomes Active and takes over the VPN connection. Router 1 comes up after manual reload and then reloads again by itself. When router 1 comes up after the second reload, SPIs are not replicated from Active router 2.

  Conditions: This symptom occurs when IPsec Stateful failover is configured on Cisco IOS Release 15.2(4)M1. This issue is seen when the HW crypto engine is enabled.

  Workaround: There is no workaround.

- CSCud79391

  Symptom: Some AVC functions (performance monitor and media-net) are missing from the advipservices image. They are included only on the adventerprise image.

  Conditions: After loading an advipservices image, some AVC functionality could not be configured.

  Workaround: There is no workaround.

- CSCud12022

  Symptom: The over-subscription of a SPA buffer causes a message to be logged; indicating packet drops in the SPA.

  Conditions: This issue occurs during re-configuration, flow-control is not set correctly on the ESP and results in a broken flow-control on the interface that is re-configured.

  Workaround: There is no workaround.

- CSCud14033

  Symptom: Traceback appears and the packet is dropped with uRPF specific cause.

  Conditions: This issue occurs when the uRPF and ACL configurations are removed and added while the traffic is running, copy **remove_config running** and copy **add_config running**.

Workaround: There is no workaround.

- CSCud16127

  Symptom: The CPC request message is passed by AIC and sent to another side.

  Conditions: The issue occurs because of an invalid IMSI.

  Workaround: There is no workaround.

- CSCud16274

  Symptom: The CPP is crashed with core dump file and traceback.

  Conditions: The issue occurs when the session setup rate is 10.

  Workaround: There is no workaround.

- CSCud21267

  Symptom: Accesses to the midplane EERPOM or power supply may fail.

  Conditions: The issue occurs when the systems have dual RPs.

  Workaround: There is no workaround.

- CSCud21578

  Symptom: The ASR 1000 router with iWAG feature running Cisco IOS Release 15.1(3)S may fail to establish a GTPv1 tunnel with ASR 5000 platform if MSISDN is not provided in the required format, that is with leading 19.

  Conditions: This failure occurs when the MSISDN in cisco-msisdn attribute from AAA server does not have 19 as Numbering Plan Indicator and Nature of Address for GTPv1.

  Workaround: Provision at AAA server to send MSISDN with first two digits as 19.

- CSCud22437

  Symptom: An ASR 1K might experience a watchdog crash due to a kernel panic. After viewing the plaintext contents of the resultant kernel core file that is generated, iosd generates a watchdog because of a soft lockup that prevents it from responding within 60 seconds: `<3>BUG: soft lockup - CPU#0 stuck for 61s! [linux_iosd-imag:26869]`

  Conditions: There is no particular condition.

  Workaround: There is no workaround.

- CSCud24321

  Symptom: The interface hierarchy gets corrupted during OIR such that subsequent reconfiguration events lead to a system crash.

  Impacted Platforms: ESP-100 and VXE-2, also known as Yoda platforms.

  Not Impacted Platforms: All CPP10 platforms, that is, ESP-10, ESP-20, ESP-40, etc. It also does not impact overlord and ultra

  Conditions: The issue occurs when:

  - The FRF.12 P3 queue is not removed from the interface during OIR
  - The code assumes all features have been removed from the interface before the default queue is removed.
  - The default queue is re-added while the P3 is already active and its sub-hierarchy is built on top of the leaf node for the P3 queue. This causes the hierarchy to grow exponentially to a point where programming the hardware fails.

Workaround: Removing the FRF.12 before OIR and reapplying it after OIR should work whether done manually or through a script. However, it is unreliable in the real world where OIR could occur due to swapping out one SPA for another unless the user remembers to disable FRF.12 before swapping the SPAs.

- CSCud24885

  Symptom: When some drops are seen: **FirewallInvalidZoneable**.

  Conditions: The issue occurs when the ASR with WCCP, ZBF, and netflow are configured at the same time.

  Workaround: Ping the destination on Cisco ASR1000 series router before introducing the WCCP traffic.

- CSCud30024

  Symptom: Packet drop may be observed during IP Security (IPSec) rekey.

  Conditions: The issue occurs on a Cisco ASR1000 series router when it functions as an IPSec termination and aggregation router, and when Internet Key Exchange version 2 (IKEv2) is used. The packet drop, due to invalid SPI, may occur on responder router during rekey.

  Workaround: There is no workaround.

- CSCud31542

  Symptom: The DHCP reply message is dropped in the data plane after RPSO or clear IPv6 neighbor.

  Conditions: The issue occurs during the following conditions:

  - Setup of DHCPv6 binding.
  - Clear IPv6 neighbor or RPSO and without traffic before adjacency convergence, then DHCP reply message will be dropped in the data plane.

  Workaround: There are several workarounds:

  - Send downstream traffic to client which will relearn the neighbor.
  - Clear IPv6 route `X::X/prefix <dhcp installing route>` to relearn the neighbor.
  - Client can reconnect after the DHCP session is timeout.
  - Client can send RS or NS.

- CSCud34131

  Symptom: ERSPAN can only monitor ZBFW interface Rx packets.

  Conditions: The issue occurs when ERSPAN packets are dropped if the ERSPAN output interface is not in the same zone as that of monitor interface.

  Workaround: Configure the ERSPAN output interface in the same zone as that of monitored interface.

- CSCud35550

  Symptom: Many trace backs are printed in the console when GTPv2 messages are handled.

  Conditions: Attached configuration is imported. It can also be triggered, if layer 7 drop is configured.

  Workaround: There is no workaround.

- CSCud35735

  Symptom: ucode along with fman_fp core seen in UUT with **GTP_AIC_FUNC_POLICY_CHANGE.**

Conditions: The issue occurs while sending traffic from SGSN.

Workaround: There is no workaround.

- CSCud37568

  Symptom: Memory leak in GTP PDP pool.

  Conditions: The issue occurs when GTP AIC is configured.

  Workaround: There is no workaround.

- CSCud37921

  Symptom: Communication broken. Update PDP Context Requests are dropped, if GSN address is not identical with the GSN address provided in Create PDP Context Request.

  Conditions: The issue occurs during the 3GPP communication on GRX interface. Roaming mobile users from GRX to inside can have different GSN address information.

  Workaround: There is no workaround.

- CSCud38010

  Symptom: Due to the change of CSCud35735: ASR1K: ucode crash at **gtp_aic_match_policy**. It is a defense for **smtp aic**, as the function call **re_multi_match_ascii** can result in crash.

  Conditions: The issue occurs when the function **re_multi_match_ascii** meet some invalid array address, which will return **0xFFFFFFFF** as the match length, here in **smtp aic**, it must be protected from this exception.

  Workaround: There is no workaround.

- CSCud38558

  Symptom: The two causes are:

  - Might be no monitoring.
  - Trackback message appears in log: **1#7e4ed294e9cee774e6d357fbecf1228d errmsg:CB20000 2230 cpp_common_os:D1AD000 BBB0 cpp_common_os:D1AD000 B9C0 cpp_common_os:D1AD000 1903C cpp_fnf_svr_lib:FE68000 15D64 cpp_fnf_svr_lib:FE68000 1C2D0 cpp_fnf_svr_lib:FE68000 18E84 cpp_common_os:D1AD000 10A94 cpp_common_os:D1AD000 110CC evlib:CEF1000 E0DC evlib:CEF1000 104C4 cpp_common_os:D1AD000 127E8:10000000 4710 c:A526000 1E938 c:A526000 1EAE0.**

  Conditions: The issue occurs:

  - On 3.8 Ver: Happens randomly if HTTP tool is deployed several times.
  - On 3.7 Ver: Happens randomly if AVC1.5 tool is deployed several times.

  Workaround: Reapply the configuration.

- CSCud39324

  Symptom: Due to the reloading of the ESP.

  Conditions: The issue occurs when the ASCII ALG traffic requiring TCP seq or delta fixup on payload length change due to address translation. This reload could occur rarely with very long lived TCP connections.

  Workaround: Turn off the ALG that is causing the issue.

- CSCud39590

  Symptom: This is a new feature for dummy packet support.

Conditions: There is no particular condition.

Workaround: There is no workaround.

- CSCud40015

  Symptom: The client or server IPs are interchanged in command **sh serv-in statis conn** on Peer ACs.

  Conditions: The issue occurs when the client or server IPs are interchanged in CLI **sh serv-in statis conn on Peer AC's.** When there are 4 AC's in an ACG and the context is up and operational, some traffic is sent and only one AC owns that flow. If the command **sh service-inse statis conn** is executed on the AC which owns the flow, it shows the right output. But when the same command is executed on the other AC's the client and server IP's are interchanged.

  Workaround: There is no workaround.

- CSCud41480

  Symptom: The QFP is reloaded.

  Conditions: The known conditions for this are to have one Firewall and NAT configured on a ASR1002-X, but crash is intermittent.

  Workaround: There is no workaround.

- CSCud41501

  Symptom: The first and last timestamps shown in the output of **show flow monitor <name> cache** command shows incorrect values on an ASR1K with RP1 route processors.

  Conditions: The following are the conditions for this symptom:

  – Attach a record that contains **timestamp sys-uptime first** and / or **timestamp sys-uptime last** field(s) to a monitor. Predefined records such as **netflow-original** already have these fields defined.

  – Under the interface config mode, configure the above defined monitor using **[ip | ipv6 | mpls] flow monitor <name> (sampler) [input | output].**

  – Issue the following show command **show flow monitor <name> cache** to see the cached records.

  – In the output of the above show command, the values displayed for the first and last timestamp fields can be incorrect.

  Workaround: There is no workaround.

- CSCud42919

  Symptom: FP crash.

  Conditions: The issue occurs when there is 70~80K translation sessions, SIP and H323 mixed traffic.

  Workaround: There is no workaround.

- CSCud44854

  Symptom: The Hash table has not been memset for ALG during initialization.

  Conditions: The issue occurs during the following conditions:

  – start **sip/h323/...** traffic

  – Established NAT session over 60~70K

  – Send CLI combinations with below actions:

  • clear **ip nat trans ***

- shutdown inside or outside traffic interfaces
- remove **nat/alg** config
- reconfig **nat/alg** and unshut interfaces

Workaround: There is no workaround.

- CSCud45750

  Symptom: Extended data forwarding outage when MLPPPOLNS session is forwarded to a new link due to a OSPF link.

  Conditions: The issue occurs when the MLPPPOLNS session is defined using a member link session with multiple paths to the destination LAC through OSPF, if the member link session interface changes after the session is active, a extended data forwarding outage may occur due to the OSPF link change. Possible MLPPP member link session flap may also occur.

  Workaround: There is no workaround.

Note Currently, only **per destination packet load balancing** is supported.

- CSCud47046

  Symptom: No-way voice occurs after transferring external calls to an external recipient. The PBX does a external transfer and uses a new transaction leg which indicates that media should be hair pinned on the SBC, but no media is heard.

  ```
  PBX(A)----SIP-----SBC(B)----SIP-----service-provider(C)
  ```

  The following are the different Call Scenario:

  - PBX(A) user dials external party (towards C) the calls is answered.
  - PBX(A) user presses the conference/transfer key which places the call on hold. MOH is heard by the external party.
  - PBX(A) user dials external party (towards c) and the call is answered.
  - PBX(A) user completes the call transfer.
  - The call transfer is completed, but no audio is heard, by either A or B.

  Conditions: The issue occurs only when all of the below conditions happen together:

  - One side has **nat** enabled and **rtp** comes before **sdp** offer/answer is completed.
  - Four calls are modified to two hair pin call sets, that is two calls are hair pined.
  - Later call modification makes four calls hair pined together.

  Workaround: There is no workaround.

- CSCud49494

  Symptom: While receiving the udp fragmented packets, ESP is crashed with multicast service reflect being configured.

  Conditions: The issue occurs when the multicast service reflect is configured and udp fragments are received in the VIF interface.

  Workaround: There is no workaround.

- CSCud49777

Symptom: In a Flex scale setup, few of the framed routes do not get installed even though all the sessions come up fine. As a result, traffic flow is affected.

Conditions: The issue occurs while clearing the crypto session on the headend. Sessions will be triggered again from SVTI. For few of the sessions, framed route is not installed.

Workaround: There is no workaround.

- CSCud50827

  Symptom: The protocol pack upgrade or loading fails, with the following error message: **failed add new signature to heuristic signature**.

  Conditions: The issue occurs during the simple protocol pack upgrade, path (starting PP 3.1).

  Workaround: There is no workaround.

- CSCud51361

  Symptom: The FNF monitor with application name key does not report HTTP host name.

  Conditions: The issue occurs in the FNF monitor with **match application name account-on-resolution**.

  Workaround: There is no workaround.

- CSCud53401

  Symptom: The router crashes due to a hardware interrupt.

  Conditions: The issue occurs when the FRF.12 is configured on ESP100 or 1RUVE2, the recycle queue cannot be changed on-the-fly because of the packets in-flight that is enqueued to this queue by the hardware.

  Workaround: There is no workaround.

- CSCud58038

  Symptom: The router crashes due to a hardware interrupt.

  Conditions: The issue occurs during the following conditions:

  – setup **sip/h323** traffic
  – shut and unshut **clear ip nat tr ***
  – remove **ip nat**, **shut clear ip nat tr ***

  Workaround: There is no workaround.

- CSCud60014

  Symptom: The control process crashes during reconfiguration on ESP100 or 1ruve2.

  Conditions: The issue occurs during the reconfiguration such as adding a hierarchical policy to an ATM, changing a class-of-service for an ATM VC, and so on, which results in a new scheduling hierarchy.

  Workaround: There is no workaround.

- CSCud61316

  Symptom: The vTCP reset storm is observed in NAT/ALG back-to-back deployment.

  Conditions: The issue occurs during the following conditions:

  – A TCP NAT session is established between two ASR1K.
  – Abnormal ALG packets are received from both the sides.
  – An additional TCP segment is received by ASR 1K after ASR1K sends out the TCP RST.

Workaround: Manually clear the affected NAT session.

- CSCud66316

  Symptom: Log messages for **REJECT Create Session Response** is not printed in **sys-log**.

  Conditions: The issue occurs when the GTP AIC is configured in the UUT.

  Workaround: There is no workaround.

- CSCud67970

  Symptom: Provisioned QoS service is not honored.

  Conditions: The issue occurs when the fair-queue is removed from the class on-the-fly, the rates, that is, bandwidth and shape, are no longer configured in the hardware.

  Workaround: Remove the fair-queue class and re-add it without the fair-queue.

- CSCud70243

  Symptom: Some IPv6 subscribers fail to come up in a scenario in which there is a frequent session churn.

  Conditions: The issue occurs on an ASR 1K router, for IPv6 subscribers that have traffic classes configured. It occurs when the sessions are torn down soon after coming up. It can also involve a change to a session's complement of traffic classes shortly after coming up, but before being torn down. A number of pending objects can register in the output of the **show platform software object-manager fp active statistics** command.

  Workaround: Remove the pending objects by performing an FP switchover on ASR 1K routers that have two of them. Before performing an FP switchover, make sure that there are not any pending objects on the standby FP. This can be determined by using the command **show platform software object-manager fp standby statistics**. If the standby FP has pending object counts when the system is in steady-state, it should be reloaded and checked for pending objects after it comes back. If the new pending object counts reach is **0**, then proceed with an FP switchover.

- CSCud72509

  Symptom: The ESP100 is crashed.

  Conditions: The issue occurs when the NAT is configured, TCP segments size is larger then 26K, ESP100, or 1002-X.

  Workaround: Add **no payload-option** in the nat entry to disable all alg or disable a specific DNS tcp alg by using the command **no ip nat service dns tcp**.

- CSCud73594

  Symptom: The MMA objects are not removed after policy detach. This is seen with the following CLI command: **show platform software object-manager fp active object-type-count | inc mma**. Eventually, this can lead to a failure in applying a Seawolf configuration.

  Conditions: The issue occurs during the massive sequence of policy attach or detach operations.

  Workaround: There is no workaround.

- CSCud73599

  Symptom: No records are generated after several configurations.

  Conditions: The issue occurs when there is a config replace or any other massive performance policy configurations.

Workaround: There is no workaround.

- CSCud73600

  Symptom: The FP is crashed.

  Conditions: The issue occurs when the QoS is configured on physical interface which is bind to a BDI interface. Stile is configured on the same BDI interface.

  Workaround: There is no workaround.

Note Stile is not supported on BDI interfaces and must not be configured on it.

- CSCud73652

  Symptom: Incorrect MMON/ART metrics reported and/or crash.

  Conditions: The issue occurs in some rare cases, when:

  – Packets of the same flow are processed by FME on more than one interfaces.

  – FME processes from the second interface and continues further, ends due to some error (rare case).

  Workaround: There is no workaround

- CSCud75024

  Symptom: The ESP **cpp_cp_svr process** crashes, with the trace back pointing to the **cpp_ess_ea_ffr_entry_free** function.

  Conditions: The issue occurs during the session teardown.

  Workaround: There is no workaround.

- CSCud77695

  Symptom: The security policy is not downloaded to the data path correctly.

  Conditions: The issue occurs on a Cisco ASR1000 series router when it functions as an IP Security (IPSec) termination and aggregation router, and when IPv6 static crypto map with large Access Control list Elements (ACEs) are configured within a single Access Control list (ACL).

  Workaround: The issue can be avoided by:

  – Applying the IPv6 static crypto map with initial ACL containing less than 10 ACEs.

  – Adding the ACEs, one-by-one, into the ACL configuration.

- CSCud78618

  Symptom: Crash.

  Conditions: The issue occurs when the iVRF is configured on the ike profile.

  Workaround: There is no workaround.

- CSCud78649

  Symptom: An error message **SBC: SBC ^T^U^\V** is not configured is printed when activating **sbc**.

  Conditions: The issue occurs when the **activate** command is Run just after the command **media-address ipv4...**

```
ASR-1001-CCN-7(config)#sbc test ASR-1001-CCN-7(config-sbc)#sbe
ASR-1001-CCN-7(config-sbc-sbe)#media-address ipv4 1.20.0.2 vrf vrfa
ASR-1001-CCN-7(config-sbc-media-address)#activate SBC: SBC ^A^T not configured.
```

Workaround: exit **sbc**, and enter **sbc** again, then Run the **activate** command.

- CSCud79391

  Symptom: The AVC functionality (performance monitor and media-net) is missing from advipservices image. It was only present in adventerprise.

  Conditions: The issue occurs when loading an advipservices image, AVC functionality can not be configured.

  Workaround: There is no workaround.

- CSCud80832

  Symptom: The ASR 1000 router can result in a ucode crash when the box is running NAT with **oer** keyword and also running PfR.

  Conditions: The issue occurs when the NAT is configured with the **oer** keyword on NAT mapping and PfR is used for traffic optimization, doing a **shut** or **no shut** on a PfR external link also happens to be the NAT outside interface, which can result in a crash if the traffic is flowing.

  Workaround: Avoid doing a manual **shut** or **no shut** on the PfR external interfaces when running with NAT. If you must do a **shut** or **no shut**, shut down the NAT inside the interface first, then do a **clean ip nat trans *** and then shut the PfR interface.

- CSCud86240

  Symptom: The ASR1K ESP crashes (ucode core file created) when compressed packets are sent on a Multilink PPP interface using IOS XE 3.5 and earlier ASR1K software images. On IOS XE3.6 and later ASR1K software images a crash does not occur, but routed traffic on configured interfaces are not forwarded. But, local traffic between the peer routers can be forwarded. In all releases, routed traffic will be dropped on any other interfaces (for example, PPP, Multilink PPP, HDLC, and so on.) configured for this mode of compression.

  Conditions: The issue occurs if the legacy IOS compression feature **compress [mppc | stac | predictor]** is configured on any interface (for example, PPP, Multilink PPP, HDLC, and so on.). If this feature is configured on a Multilink PPP interface then the ESP crash can be encountered if using an IOS XE3.5 or earlier ASR1K software image.

  Workaround: Remove the compress **[mppc | stac | predictor]** feature configuration from all interfaces as this functionality is not supported on the ASR1K. The software fix associated with this bug report will be removing this configuration option from the ASR1K.

- CSCud88366

  Symptom: Kingpin: plim tx drop if gi0/0/0 is used as tunnel source physical interface.

  Conditions: The issue occurs when Gige interface as SVT tunnel source interface and 4K QoS policy is applied to 4K SVTI tunnel.

  Workaround: There is no workaround.

- CSCud88517

  Symptom: The system is out-of-service.

  Conditions: The issue is observed on a Cisco ASR1000 series router when it functions as an IP Security (IPSec) termination and aggregation router, and when more than 30 IPSec sessions are up and running traffic.

  Workaround: There is no workaround.

- CSCud90021

  Symptom: An ASR1K running **03.06.00.S.152-2.S** can crash due to a NAT bind age timing.

Conditions: This issue is a rare timing condition which is triggered by the RG infra toggle.

Workaround: There is no workaround.

- CSCud90142

  Symptom: The GTPv2 drop counter increments, when actually, no messages are dropped.

  Conditions: The issue occurs when the cause value in Create Session Response is 78.

  Workaround: There is no workaround.

- CSCud91102

  Symptom: Router reload.

  Conditions: The issue occurs during the heavy AVC traffics.

  Workaround: There is no workaround.

- CSCud91877

  Symptom: Cannot include "**.**" in the variable name, used in header editor.

  Conditions: The issue occurs always.

  Workaround: There is no workaround.

- CSCud91920

  Symptom: When configuring an ACL for both IPv4 and IPv6 in a policy-map, the policy-map does not work properly.

  Conditions: The issue occurs when an ACL is configured for both IPv4 and IPv6 in a policy-map and when the policy-map is attached to an interface or control-plane.

  Workaround: Use IPv4 ACL and IPv6 ACL in a same class-map with match-any.

- CSCud92837

  Symptom: The **aggregation-type prefix-length** of PfR cannot be configured to less than 16. If so, the number of learned prefix will be much less than what it must be.

  Conditions: The issue occurs when PfR is enabled.

  Workaround: It is better to configure the **aggregation-type prefix-length** of PfR to greater than 24.

- CSCud92879

  Symptom: The current session for control plane is too small.

  Conditions: The issue occurs during the basic GTPv1 configuration, and GTPv1 traffic.

  Workaround: There is no workaround.

- CSCue15619

  Symptom: SBC CLI hung.

  Conditions: The issue occurs while configuring the **signaling-peer-port** when the **adj** is attached, the new vty terminal would be hung.

  Workaround: There is no workaround.

- CSCue17371

  Symptom: NTE cannot pass through.

  Conditions: The issue occurs for a transcoding call.

  Workaround: There is no workaround.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8S

This section describes the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8S. It contains the following topics:

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.8S

This section documents the unexpected behavior that might be seen in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8S.

- CSCtr38540

  Symptom: In the Cisco ASR 1001 Router, false temperature readings from the power supply similar as the one displayed here, are reported:

  ```
  June 18 03:36:37.700:%ENVIRONMENTAL-1-ALERT: Temp: Inlet, Location: P1, State:
  Shutdown, Reading: 127 Celsius
  ```

  Conditions: This is seen only on the Cisco ASR 1001 Router.

  Workaround: There is no workaround.

- CSCua99781

  Symptom: The ESP gets reloaded.

  Conditions: This symptom is observed when you issue the **clear crypto session** command with the 4k IKEv2 IPv6 static crypto map tunnels and bidirectional traffic of 2Gbps 300B packets.

  Workaround: There is no workaround.

- CSCuc74857

  Symptom: NAT address pool exhaustion occurs with high DNS traffic.

  Conditions: Payload addresses in DNS PTR record natted without active NAT bindings. RFC 2694 suggests that DNS PTR queries should not be translated if no active bindings are found in the NAT translation table. Per current implementation, new NAT dynamic bindings are created when processing DNS PTR queries, eventually contributing to NAT address pool exhaustion.

  Workaround:

  - Add deny ACL to avoid NAT translation of unknown payload addresses in the DNS PTR query.
  - Turn off DNS ALG service if possible.

- CSCud00613

  Symptom: The physical interface goes down in the shutdown state when you load the configuration on a Cisco ASR 1000 Series Aggregation Services Router.

  Conditions: The IP address of default gateway under GTP should not overlap with any of the existing interface configurations. If it does, the Cisco IOS software will shut down the interfaces that have overlapping IP addresses. The iWAG creates a virtual interface based on the IP address provided under the GTP or the APN default gateway configuration as follows:

```
gtp
apn 1
default-gw 192.168.10.1 prefix-len 16 <virtual-interface will be created with ip
address 192.168.10.1>
```

Workaround: If you configure similar interfaces, you have to unconfigure the entire GTP configuration using the **no gtp** command, go to either the physical interface or the loopback interface, perform a **no shut** action, and reconfigure the interface using the **gtp** command.

- CSCud15949

  Symptom: The CPP traceback notifying monitor cannot be reserved.

  Conditions: The issue was seen when the MMA policy, mediatrace policy, and one FNF monitor were attached to an interface.

  Workaround: If the FNF monitor is configured, only one policy may be attached on the interface and direction. This should not exceed the following:

  num_of_policies*5 + num_of_fnf_monitors > 10.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.8S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.8S.

- CSCsd20055

  Symptom: The DHCP client is not installing a default route if the physical interface is assigned to a Virtual Routing and Forwarding (VRF) table.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: Manually configure a static default route in VRF.

- CSCso75347

  Symptom: When the **cable dhcp-giaddr policy strict** command is configured on the Cisco CMTS, the CPEs behind the CMs are expected to get the DHCPOFFER message with its source IP address belonging to secondary IP Network Address range of the downstream cable interface in the CMTS. Currently, the DHCPOFFER has the source IP address from the downstream's primary IP network address range.

  Conditions: The issue occurs when the **cable dhcp-giaddr policy strict** command is configured in the CMTS cable downstream interface.

  Workaround: There is no workaround.

- CSCsq83006

  Symptom: When some port channels go down at the same time on a router, it can cause EIGRP SIA errors.

  Conditions: This symptom occurs with full mesh four routers that are connected via port channels. Additionally, it occurs with over five routers that are connected via a partial mesh port channel.

  Workaround: Use the following port-channel interface settings:

  ```
  (config)# interface port-channel <port-channel-interface-number>
  (config-if)# bandwidth <bandwidth-value>
  (config-if)# delay <delay-value>
  ```

- CSCsr03117

  Symptom: The UDP direct-broadcast packets get dropped even if the ACL is configured to permit this traffic.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: Configure the ACL statement as permit ip X.X.X.X X.X.X.X host 255.255.255.255.

- CSCsv08144

  Symptom: Even if the MLPPP LFI is correctly configured on a multilink interface, the **show ppp multilink** command continues to show interleaving as disabled.

  Conditions: This symptom occurs when a Cisco ASR 1000 Series Aggregate Services Router has PPP multilink interleave configured on the multilink interface on the multilink virtual template (for broadband MLPPP).

  Workaround: The **show plat hard qfp act feat mlp data bundle** <*full-bundle-interface name*> **detail** command shows the correct status of the interleaving on the interface.

- CSCsz65576

  Symptom: One or more linecards may fail to boot in a Cisco ASR 1000 Series Aggregate Services Router with an RP2 may occur, or an error with the `EOBC. %CMFP-3-STANDBY_EOBC_LINK_ERROR: F0: cman_fp: Standby EOBC link` error detected.

  Conditions: This symptom is only seen with certain combinations of RP2 and ESP10.

  Workaround: There is no workaround, but the issue is not seen with an ESP20.

- CSCtd43540

  Symptom: A memory leak occurs at `cdp_handle_version_info`.

  Conditions: This symptom is triggered by misbehavior of peer switch running Cisco IOS Release 12.2(46)SE that has been fixed in CSCsm63025. The symptom is observed with link flapping.

  Workaround: Disable CDP on the flapping interface.

- CSCtd54694

  Symptom: A crash is seen when the **show cdp neighbor port-channel** *no* and the **show cdp neighbor port-channel** *no* **de?** commands are executed.

  Conditions: It is a rare timing issue.

  Workaround: Use the **show cdp neighbor** and **show cdp neighbor detail** command to view both the brief and detailed CDP information respectively as a workaround. Also, the **show cdp neighbor** <*interface type*> *no* command can be used except when the interface type is *port-channel*.

- CSCtd58886

  Symptom: The CMTS crashes when the SNMP client enquires `ifRcvAddressEntry` that contains a non-zero address of a GE interface in the SPA.

  Conditions: This symptom is observed on a Cisco uBR10000 Router with a 5GE SPA that runs Cisco IOS Release 12.2SCB or 12.2SCC with the following SNMP command:

  getnext -v2c <*cmts address*> [*community*] **ifRcvAddressStatus/ ifRcvAddressType**.<*ifIndex of GE in SPA.non-zero address*>

  Workaround: Do not query this entry of the table since it does not exist.

- CSCtg39957

  Symptom: Spurious memory access occurs during the `tspts_handle_rsvp_pathtail_events` function.

Conditions: This issue occurs when a PATH message without any session attribute object is being received from the TE head end. Note that the Cisco IOS and Cisco XR routers always send the session attribute object.

Workaround: There is no workaround.

- CSCtg47129

  Symptom: Memory leaks are observed on the Cisco CMTS router when NAT is configured.

  Conditions: This issue is observed in the context of packets that need NAT in a VPN Routing and Forwarding (VRF) environment.

  Workaround: There is no workaround.

- CSCth15357

  Symptom: You are allowed to configure a `max-threshold` value higher that is than the configured queue-limit even when the `max-threshold` value cannot exceed the configured queue limit value.

  Conditions: This symptom is seen in Cisco routers loaded with Cisco IOS version 15.1(2.1)T.

  Workaround: There is no workaround.

- CSCth16914

  Symptom: Allocated memory not accounted for in the MLP client.

  Conditions: This issue occurs during power up.

  Workaround: There is no workaround.

- CSCth71093

  Symptom: Routers that are configured to dump core to `flash:` or `flash0:` fail to dump correctly to the 4GB compact flash card.

  Conditions: This is observed in the `exception flash all flash` configuration.When you issue a **wr core** command, it fails to dump the core files.

  Workaround: Dump cores to the TFTP.

- CSCti31463

  Symptom: The Cisco IOS route does not store more than two classless static routes learned through DHCP option 121.

  Conditions: Current implementation supports only two static routes.

  Workaround: Statically configure the routes.

- CSCti62247

  Symptom: If an IPv4 or IPv6 packet is sent to a null interface, a Cisco ASR 1000 Aggregation Services Router does not respond with an ICMP or ICMPv6 packet.

  Conditions: This symptom occurs with a prefix routed to the Null0 interface.

  Workaround: There is no workaround.

- CSCtk15666

  Symptom: Cisco IOS password length is limited to 25 characters.

  Conditions: Cisco IOS password length is limited to 25 characters on NG3K products.

  Workaround: There is no workaround.

- CSCto43670

Symptom: The Cisco ASR 1000 Aggregation Services Router crashes while running the **show running-config** command after configuring the replicate route with forward-referenced VRFs.

Conditions: This issue occurs only when route-replicate configurations include forward-referenced VRFs, that is, VRFs are not defined at the time of route-replicate configuration, and the replicate route is configured using the **topology** subcommand of the **global-address-family ipv4 multicast** command.

Workaround: Run the **show running-config** command after defining the forward-referenced VRFs.

- CSCto73799

  Symptom: Standby RP bulk synchronization modifies certain multiline commands in the process of loading the active RP running configuration.

  Conditions: Banner and refuse message commands that have the opening ^C on the command line followed by some characters before the first new line and further input, can result in the standby inserting an extra new line into the standby configuration between the ^C and the content that is supposed to appear on the first line. The **shell map** and **macro auto** commands that have multiple unmatched closing braces in their multiline input will be misread, such that the resulting command is interpreted by the standby as invalid. If the active is configured to reload the standby on invalid commands, the standby RP will be reloaded as a result.

  Workaround: Format the commands in such a way that these conditions are avoided. If the chosen formatting produces visible symptoms on the standby, adjust the formatting, save the configuration, reload the standby and verify that the symptoms have been cleared from the standby's running-configuration.

- CSCto75838

  Symptom: Opening client sockets to IPv4 addresses fail with an invalid argument error message.

  Conditions: This issue only occurs with IPv4 sockets. IPv6 sockets work properly.

  Workaround: Use the IPv6 client connections.

- CSCto87436

  Symptom: Under certain conditions, Cisco IOS devices may crash, and the following error message appears:

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

  Conditions: If an SSH connection to a Cisco IOS device is slow or idle, it may cause a box to crash with an error message.

  Workaround: There is no workaround.

- CSCtq24011

  Symptom: Routers behave in a way similar to when a local-proxy-arp is configured on them and perform a proxy-arp even for the systems in the same subnet.

  Conditions: This issue occurs when the Cisco ASR 1000 Aggregation Services Router receives an ARP request on an interface when the interface is not fully initialized, and the connected routes are not added to the routing table yet. This causes the proxy-arp reply and wrong arp entry to freeze.

  Workaround: Perform **shut** or **no shut** on victim and offender routers.

- CSCtq64716

  Symptom: The following warning message may be displayed during router boot even when the server is defined: `%RADIUS-4-NOSERVNAME`

  Conditions: This symptom is not caused by any specific condition.

Workaround: There is no workaround.

- CSCtq94843

  Symptom: An IP prefix list entry exists even after unconfiguring the prefix list.

  Conditions: This issue is seen when a prefix list that is the last one being configured is deleted by deleting individual entries. However, the prefix list can still be displayed with **show** commands.

  Workaround: Configure a new prefix list or an existing prefix list.

- CSCtr45030

  Symptom: The SNMP timers causes the Cisco ASR 1000 Aggregation Services Router to exit the global configuration mode or prevents the console from entering the global configuration mode.

  Conditions: Occurs when you copy and paste large configurations, particularly a large number of VLAN configurations. The issue occurs without any SNMP configurations present.

  Workaround: Perform the following workarounds:

  - Disable RMON.
  - If the configuration is huge, paste in multiple blocks.
  - Enable SNMP timers. Paste the required configuration when the timer callbacks have finished executing.

- CSCtr45978

  Symptom: The Cisco IOS WAAS contains FTP or HTTP connections that are hung in the CONN_ABORT state.

  Conditions: If the Cisco ASR 1000 Aggregation Services Router is configured with Cisco IOS WAAS, the FTP packets or real HTTP user traffic to web sites is through the WAN link.

  Workaround: There is no workaround.

- CSCtr74577

  Symptom: A traceback is seen at the coa_ha_proc_qos_template with lawful intercept using SNMP on L2TP sessions.

  Conditions: This issue is seen in the Cisco ASR 1000 Aggregation Services Routers that have been configured for lawful intercept on L2TP sessions.

  Workaround: There is no workaround.

- CSCtr96024

  Symptom: A user is not notified about an error scenario relating to larger-than-allowed flow record of type performance-monitor being used in a performance monitor policy. This is misleading because the user may believe that the performance monitor policy is correctly attached to the desired interface, but will find that the task of monitoring traffic is not working as expected.

  Conditions:

  The symptom is observed under the following conditions:

  - The Performance Monitor feature is being used on the Cisco ASR platform.
  - A flow record of the performance-monitor type, which contains more than the maximum allowed fields, has been configured.

  - The user is referencing the performance-monitor type flow record in a performance monitor policy that has been attached to an interface. The maximum number of fields allowed in a flow record is 32 in the **timestamp sys-uptime first** and **field timestamp sys-uptime last** fields. If the timestamp fields are absent, they are automatically added to the record. However, the total number of fields should still be less than or equal to 32.

  Workaround: Use a flow record of type performance-monitor having 32 or less fields.

- CSCts00341

  Symptom: While executing a CLI that requires a domain name lookup such as **ntp server** *server.domain.name*, the command fails, and the following error message appears:

  ```
  DNS is not resolved with dual RPs on ASR1k Translating server.domain.com ...domain
  server (10.1.1.1). Standby doesn't support this command. Invalid input detected at
  '^' marker.
  ```

  Condition: This issue is observed when a redundant RP chassis is operating on the SSO mode.

  Workaround: Instead of using *hostname* in the command, specify the IP address of the host. In some scenarios, this could cause the standby SUP to crash without a crash file. Remove the host names that require DNS lookup and use their IP addresses instead.

- CSCts02777

  Symptom: Command attributes are sent multiple times in AAA command authorization and accounting requests.

  Conditions: Seen in Release 15.0(1)S when TACACS command authorization or accounting or both are configured.

  Workaround: There is no workaround.

- CSCts44393

  Symptom: A Cisco ASR 1000 Series Aggregation Services Router crashes during a BGP stress test.

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

  Workaround: There is no workaround.

- CSCts46825

  Symptom: The execution of the **mtu** command within XConnect submode can, under certain preconditions, match and run in the interface mode due to a parser cache entry existing and being previously used from the XConnect submode's parent mode (service instance mode).

  Conditions: The problem is generic to the parser cache, although we have no externally reported cases, and the preconditions are rare.The preconditions for triggering this issue include having identical commands in both a configuration submode and a grandchild submode of that submode as well, and then executing a sequence of commands that allow the system to create a cache entry for the submode instance of the command (this is normal), and subsequently (by repeating the subject command while in the child submode) learn that the child submode is a valid user of this same cache entry, and then finally attempt the identical command from the grandparent submode where the system thinks it can use the cache entry.

  Workaround: Since the bug causes the command to execute in a mode other than the target mode, that command's change needs to be reversed, and then, after executing the **clear parser cache** command, you can repeat the command from the desired submode. Another workaround is to add a few spaces to the end of the grandchild submode command before execution, to avoid the above cache entry due to mismatched input.

- CSCts52120

  Symptom: Traceback found for PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT.

  Conditions: RPSO.

  Workaround: There is no workaround.

- CSCts54641

  Symptom: Various small, medium, or big VB chunk leaks are seen when polling the EIGRP MIB and during an SSO.

  Conditions: This issue is observed when MIBs are being polled or duing an SSO.

  Workaround: There is no workaround.

- CSCts55778

  Symptom: A problem involving two SAF forwarders occurs, with one running EIGRP rel8/Service-Routing rel1 and the other running EIGRP dev9/Service-Routing dev2. The capabilities manager, a client of the service-routing infrastructure, advertises two services. When forwarders are peering with the same release image, the services propagate between the forwarders without any problems. However, when you run rel8/rel1 on one forwarder and dev9/dev2 on the other forwarder, a third service appears in the topology table along with the SR database that was not advertised. The problem cannot be re-created if both the forwarders are running an Cisco IOS XE Release 3.4S or and Cisco IOS XE Release 3.5S image.

  Conditions: This issue occurs when two SAF forwarders peer with each other using different release versions of the EIGRP SAF forwarder.

  Workaround: Make sure that each EIGRP SAF forwarder is using the same image release.

- CSCts64346

  Symptom: The **bgp nexthop route-map** command does not work with many IPv6 and IPv4 next hops under IPv6 AFs.

  Conditions: When the IPv6 Next Hop track is enabled by default, we need a way to filter some next hops for not being tracked. The **bgp nexthop route-map** command does not work with many IPv6 and IPv4 next hops under IPv6 AFs.

  Workaround: Disable IPv6 NHAT.

- CSCts68626

  Symptom: PPPoE discovery packets cause packet drop.

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

  Workaround: There is no workaround.

- CSCtt14747

  Symptom: When you issue the **shut** or **no shut** commands on the APS active box, it triggers a switchover, and VCs are not getting provisioned on the new inactive box.

  Conditions: IMA interface of Ceop SPA for port mode cell relay.

  Workaround: There is no workaround.

- CSCtt15090

  Symptom: In an MVPN environment, the VRF Route Import Extended Community (RFC 6514) is not getting attached to VPN routes.

  Conditions: The Router BGP is configured before the MDT is configured on the VRF.

Workaround: Perform a soft clear.

- CSCtt15472

  Symptom: The following error message is displayed while the SPA is booting up during OIR in the IMA PVP mode: `SPA_PLIM-3-ERRMSG`

  Conditions: This issue is seen on the IMA interface of the CEOP SPA for the PVP mode cell relay during SPA or line card OIR.

  Workaround: There is no workaround.

- CSCtt19856

  Symptom: On the Cisco ASR 1000 Series Aggregation Routers, when making changes to the **ppp multilink fragmentation** *size* command on the virtual template, the resulting change is reflected in the active bundles of the Cisco IOS software. However, the QFP does not reflect this change. The MLPPP fragment size remains at the previous setting, potentially impacting the performance and operation of the network.

  Conditions: This issue occurs when the MLPPPoBB subscribers will have the **ppp multilink fragmentation** *size* command set on the virtual template and its size value is altered.

  Workaround: MLPPPoBB subscribers using a virtual template that is changed should be flapped to pick up the new value.

- CSCtt21228

  Symptom: The Cisco ASR 1000 Series Aggregation Router crashes while trying to configure the TCL script the SSH connection.

  Conditions: SSH to the router and then try to configure the TCL script.

  Workaround: There is no workaround.

- CSCtt37115

  Symptom: The RADIUS server does not come up during the TGN session.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: There is no workaround

- CSCtt42922

  Symptom: TCP half close fails on the server side.

  Conditions: When you perform a TCP half-close session, it fails.

  Workaround: There is no workaround.

- CSCtt45381

  Symptom: Cisco IOS software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the Cisco ASR 1000 Series Aggregation Router to leak memory or to reload. Cisco IOS software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.

  Conditions: An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.

  Workaround: Cisco has released free software updates to address these vulnerabilities. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

- CSCtt95505

  Symptom: The Cisco ASR 1000 Series Aggregation Router crashes after the OSPF routing protocol is configured.

  Conditions: The crash occurs after the OSPF with a summary prefix is configured with a summary prefix, unconfigured, and configured again.

  Workaround: There is no workaround.

- CSCtt95532

  Symptom: The QL status changes to QL-INV0 the network clock is configured.

  Conditions: The QL-Value changes to QL-INV0 after the POS interface for network clock input is reconfigured

  Workaround: There is no workaround.

- CSCtu07968

  Symptom: A Cisco 890 router may provide incorrect performance monitor statistics and omit some incoming packets from being handled by flexible netflow.

  Conditions: This is observed when performance monitoring or Cisco IOS Flexible Netflow is enabled with IPsec over a tunnel on an input interface.

  Workaround: There is no workaround.

- CSCtu16862

  Symptom: L4F tracebacks are observed with SMB stress test traffic. You may experience a couple of retransmissions due to that along with some small performance degradation.

  Conditions: The symptom is observed with stress testing.

  Workaround: There is no workaround.

- CSCtu25952

  Symptom: One multicast packet is forwarded on (*,G) even though (S,G) exist in the mroute table.

  Condition: A PIM neighbor goes down between a CE and a PE in an mVPN environment or on any link between routers on both the RPT and SPT for a given PIM SM source.

  Workaround: There is no workaround.

- CSCtu28382

  Symptoms: The SIP-200 line card crashes after a switchover with multilink configurations.

  Conditions: This symptom occurs after switchover with multilink configurations.

  Workaround: There is no workaround.

- CSCtu28696

  Symptom: A Cisco ASR 1000 Series Aggregation Services Router crashes with **clear ip route ***.

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

  Workaround: There is no workaround.

- CSCtu36446

  Symptom: The following error messages are displayed during a performance test with greater than 20 CPS using the Cisco Radclient callsPerSecond Tool:

```
Nov 10 12:56:32.953 EDT:
%FMANRP_ESS-4-SESSCNT: ESS Provision Lterm Session: Unsupported peer_segtype= (0x15)
Nov 10 12:56:32.955 EDT: %FMANRP_ESS-4-WRNPARAM_U: Get Lterm Peer ESS Segtype:
Unsupported Peer SEGTYPE= (21) Nov 10 12:56:32.956 EDT: %FMANRP_ESS-4-WRNEVENT2:
Ignoring Invalid ESS Segment: ESS segment/signature (0x0 / 0x0) Nov 10 12:56:32.957
EDT: %SW_MGR-3-CM_ERROR_CLASS: Connection Manager Error: Class ADJ: - unable to unbind
segment 2. Nov 10 12:56:32.958 EDT: %SW_MGR-3-CM_ERROR: Connection Manager Error -
unprovision segment failed [ADJ:Lterm:43232] - hardware platform error.
```

Conditions: This symptom is observed in high-scale and iEdge sessions.

Workaround: There is no workaround.

- CSCtu60206

  Symptom: The upstream multicast hop (RFC 6513) installed in the muRIB is not correct.

  Conditions: The PIM is not enabled on any VRF interface. This is also a timing issue, and is more likely to occur when the router first boots up.

  Workaround: Perform a hard clear of the BGP session. Further Problem Description: At this time, the upstream multicast hop that should be installed is the one with the highest router ID.

- CSCtu83138

  Symptom: Tracebacks %AAA-3-BADLIST: invalid list AAA ID at stby-RP during session churns

  Conditions: This issue occurs when tracebacks are logged at a standby RP when flapping 8000 PTA sessions with 3 QoS services and ISG TCs (both v4 and v6) with accounting enabled and subscriber accounting acccuracy disabled.

  Workaround: There is no workaround.

- CSCtu85474

  Symptom: If the router is booted with no configuration, the ldp_api_discovery_request_async() and lcon_api_lib_path_label_notify_register() APIs return error code 2 even though the API ldp_api_app_global_is_enabled(LDP_CLIENT_ID_LCON, &is_enabled); sets "is_enabled" to TRUE.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: There is no workaround.

- CSCtv01521

  Symptom: Logs: %LSMPI-4-INJECT_FEATURE_ESCAPE: Egress IP packet delivered through legacy inject path

  Conditions: This issue occurs when Ethernet/QinQ/LCP/IP frames are received on a QinQ subinterface with PPPoE.

  Workaround: There is no workaround.

  Further information: Use the **debug platform software infrastructure inject err_packet** command to get the first 32 bytes of the packets causing this. Alternatively, use the **debug ip cef packet all input rate 10 dump** command to dump the full packets.

- CSCtw52819

  Symptom: OQD in the mGRE tunnel.

  Conditions: This symptom is observed in mGRE tunnel.

  Workaround: There is no workaround.

- CSCtw53516

  Symptom: L-bit is not set in the SATOP E3 unframed mode.

Conditions: Do shut on the interface on CE1.

Workaround: There is no workaround.

- CSCtw62695

  Symptom: Packets sent by the Cisco IOS NTP server will have the IP Identification field set to zero, a behavior that may be flagged as a vulnerability by some security scanners.

  Conditions: This issue occurs when NTP server is configured on Cisco IOS software.

  Workaround: There is no workaround.

- CSCtw76127

  Symptom: During the shutdown of a TCP connection, an erroneous **`bad seg`** error message may be displayed, and a TCP reset (RST) sent.

  Conditions: The issue occurs when a TCP connection is closed.

  Workaround: There is no workaround.

- CSCtw80336

  Symptom: Simultaneous PE reloads causes the standby pseudowire to go down.

  Conditions: This issue occurs when the CRoMPLS port mode with backup peer and cell packing is configured.

  Workaround: There is no workaround.

- CSCtw87132

  Symptom: A Cisco 2921 Router may crash when clearing a TCP session.

  Conditions: The issue has been experienced on the Cisco 2921 Router that is running Cisco IOS Release 15.1(4)M through to Release 15.1(4)M3.

  Workaround: There is no workaround.

- CSCtw88090

  Symptom: On the ASR1004 dual software redundancy setup, with 3k vrf, 3k eBGP session and 0.75M vpnv4 prefix on ASR1001, there are 40 GRE tunnels configured between local PE and remote PE router, no mpls enabled on P router. the PE router connect to ixia directly, when reload the PE router under traffic and prefix injecting, after a couple of show commands **show ip interface brief** and **show platform**, the system crash at BGP I/O.

  Condition: The issue occurs randomly with large-scale configuration on a Cisco ASR 1004 RP2 ESP20 dual software redundancy system with a Release 15.2(02)S image.

  Workaround: There is no workaround.

- CSCtw88689

  Symptom: A crash occurs while applying a policy map with more than 16 classes with the Cisco 3900e platform.

  Conditions: This symptom occurs when applying the policy map with more than 16 classes.

  Workaround: There is no workaround.

- CSCtw93140

  Symptom: Typing **wr mem** while using an IP base or LAN base boot level of Cisco IOS-XE causes the following message to appear on the console:

  ```
  Switch#wr mem
  Building configuration...
  ```

```
% VRF table-id 0 not activeCompressed configuration from 6714 bytes to 2004 bytes[OK]
Switch#
Switch#
```

Conditions: This issue is seen only if the configuration contains an **ip vrf** or an **vrf definition** section.

Workaround: There is no workaround.

- CSCtw98200

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

  Conditions: This symptom is observed if the Cisco ASR1000 Series Aggregation Services Routers are configured as LNS. RIP is configured with the **timers basic** *5 20 20 25* command. Also, every interface matching the network statements is automatically configured using the **ip rip advertise** *5* command. These interfaces include the loopback and virtual template interfaces too. On the Cisco ASR1000 Series Aggregation Services Routers, this configuration causes the creation of full VAIs that are not supported. Hence, the sessions do not come up. On the Cisco ASR 7200 Routers, VA subinterfaces can be created.

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

- CSCtx02442

  Symptom: An attempt to set uninitialized watched boolean and corresponding traceback are observed when the standby PRE crash in ISSU runversion stage.

  Conditions:

Note 1. Single step ISSU;

2. Whenthe **issu runversion** command issued the performedis PREA reloaded and changed to stby-PRE.

3. After the PREA is reloaded successfully, the PREA crashes with an exception.

4. After the PREA reloaded successfully, a traceback is reported on PREB (Active PRE).

Workaround: There is no workaround.

- CSCtx05726

  Symptom: While creating a bulk number of traffic engineering tunnel interfaces on the router with the **tunnel mpls traffic-eng exp-bundle master** option, the standby route processor crashes.

  Conditions: This symptom is seen with a specific set of configurations that have a large number of tunnel interfaces (scale number 1000) followed by the creation of a large number of master tunnels (scale number 1000). Copying such a configuration to the router causes this crash to occur on the standby processor. The tunnel interfaces that are created at the beginning of the configuration are added as members to the master tunnels in the later part of the configuration. During this phase of creation of master tunnels and adding member tunnels, these tunnel interfaces go through a cycle of create-delete-create. When such a configuration is being synchronized to the standby route processor along with the resulting create-delete events, the standby processor crashes. This point at which the crash occurs is random and occur during the configuration of any of the master tunnels.

  Workaround: There is no workaround.

- CSCtx06018

  Symptom: The interface queue wedge is seen when performing the WAAS performance test.

  Conditions: This symptom is observed when performing the WAAS performance test.

Workaround: Increase the interface input queue hold size.

- CSCtx06801

  Symptom: Certain websites may not load or load very slowly when content scan is enabled. Delays of up to 30 seconds or more may be seen.

  Conditions: This symptom is observed when content scan is enabled.

  Workaround: Refreshing the helps sometimes, though not always.

- CSCtx06813

  Symptom: The installation fails with the rwid type l2ckt error message. Also the VC may fail to come up on the Quad-Sup router. This bug is specific to the Cisco Catalyst 6000 Quad-Sup SSO.

  Conditions: This symptom is observed in a scaled scenario, doing second switchover on Quad-Sup router.

  Workaround: There is no workaround.

- CSCtx14467

  Symptom: The ..... device crashes if kronis used to copy the configuration through the SCP and archive commands.

  Conditions: This issue occurs when the server is down or the link to server is down.

  Workaround: Manually upload the file to the server.

- CSCtx20517

  Symptom: Customers see Cisco IOS-XE fragment errors in their logs repeatedly every 30 seconds after upgrading to the asr1000rp1-adventerprisek9.03.03.00.S.151-2.S.

  Conditions: WCCP has to be enabled.

  Workaround: There is no workaround.

- CSCtx23593

  Symptom: Some virtual circuit information is missing from the cAal5VccEntry SNMP MIB object in the output of the **snmpwal** command, but not in the router configuration command.

  Conditions: This symptom is observed on a Cisco 7204VXR NPE-G2 Router that is running the 12.2(33)SRE5 (c7200p-advipservicesk9-mz.122-33.SRE5.bin) image in the customer network. This issue may also occur in other releases. This issue typically occurs over a period of time because of creation or deletion of subinterfaces. It also occurs if a customer uses the **snmp ifmib ifIndex Persist** command, which retains the ifIndicies assigned to the @~@subinterfaces across router reload.

  Workaround: The following are the workarounds:

  – Enter the show atm vc privileged EXEC command on the same device to obtain a complete list of all the VCs or perform the SNMPWALK, suffixing the ifIndex of the interface to get the value.

  – Enter the following configurations:

  ```
  no snmp ifmib ifIndex Persist
  no snmp ifindex persist
  copy running start
  reload
  snmp ifmib ifIndex Persist
  snmp ifindex persist
  ```

- CSCtx34823

Symptom: The OSPF keeps bringing up the dialer interface even after the expiry of idle timeout.

Conditions: This symptom occurs whenthe on-demand OSPF is configured under the dialer interface.

Workaround: There is no workaround.

- CSCtx38121

  Symptom: IPv6 traffic does not pass through the interface attached to a service policy matching IPv6 the traffic using IPv6 ACL.

  Conditions: This symptom is observed when attaching a service policy that matches the IPv6 traffic that is configured using ipv6 access-list on the EFP of an interface, which leads to a traffic drop.

  Workaround: There is no workaround.

- CSCtx38338

  Symptom: When a VFI is attached to a VLAN interface, it does not overwrite any of the existing VFIs.

  Conditions: This occurs when a different VFI is attached to a VLAN interface.

  Workaround: Avoid overwriting VFIs on a VLAN interface.

- CSCtx40818

  Symptom: Traffic drops in a Cisco and the following error message is displayed:

  ```
  %IP-3- LOOPPAK: Looping packet detected and dropped - src=122.0.0.11, dst=121.0.0.11,
  hl=20, tl=40, prot=6, sport=80, dport=57894
  ```

  Conditions: This symptom is observed if the WAAS, NAT, and firewall are enabled.

  Workaround: Disable the WAAS.

- CSCtx40959

  Symptom: The CPUHOG occurs.

  Conditions: This issue occurs when the configuration comprising a mesh of 17 BGP routers, with all the routers having network statements covering the IP prefixes on the 16 VLAN subinterfaces that interconnect them. When the main interface on a given router is shut, all the subinterfaces also go down, causing all the connected routes to be removed. This leads to the CPUHOG.

  Workaround: There is no workaround.

- CSCtx42223

  Symptom: The connection with an FRR client that is registered for a BFD session is lost after an SSO. FRR cut-cover time is much more than 50 ms, which is not expected.

  Conditions: This is observed after an SSO, when the FRR client is registered for a BFD session.

  Workaround: Bring down the BFD session and configure it again.

- CSCtx48753

  Symptom: Higher memory usage with PPP sessions than seen in Cisco IOS XE Release 3.4 and Release 3.5.

  Conditions: This issue is observed with configurations containing PPP sessions. Such configurations see up to 10 percent higher Cisco IOS memory usage than in previous images.

  Workaround: There is no workaround.

- CSCtx49270

  Symptom: A memory leak is observed when the Fast UDLD feature is configured on a router.

Conditions: The router must support UDLD, and the feature must also be enabled on the router using the **udld aggressive** command. The UDLD can be enabled either on individual interfaces or globally.

Workaround: The workaround is to not enable the Fast UDLD feature on the router.

- CSCtx53391

  Symptom: when the ... router is reloaded or when some interface flap events are executed.

  Conditions: When a VC bundle is configured under the same interface that has PVCS with IPv6 addresses, the Ucode crashes due to adjacency-related issues. Note that this issue is seen only intermittently.

  Workaround: Avoid configuring PVCS with IPv6 addresses and bundles under the same main interface.

- CSCtx57146

  Symptoms: SIP SPA goes out of service state in scaled sub=interface config (more than 2000 subinterface on single GigE port).

  Conditions: While performing an ISSU between the iso1-rp2 and iso2-rp2 xe3.6 throttle images after ISSU run-version, the SIP SPA goes out of service and needs a heavily scaled configuration. This issue is observed when there are 2000 to 3000 subinterfaces on a single SPA and the following limits are exceeded: overall dual stack VRFs per box; 2800 dual stack limit on interface: 1000.

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

  1. Before performing a load version from RP0 (initial active), execute the **show ipv6 route table | inc IPv6** command.

  2. Note down the number of IPv6 route tables in the system.

  3. Perform a load version.

  4. Wait for the standby to come up to Standby hot.

  5. Enable the standby console from RP0 (active) **asr1000#configure terminal**. Enter the configuration commands, one per line. End with **CNTL/Z**. a**sr1000(config)#**, **asr1000(config)#redundancy**, **asr1000(config-red)#main-cpu**, and **asr1000(config-r-mc)#standby console enable**.

  6. Log in to the standby console and execute the **asr1000-stby# show ipv6 route table | inc IPv6** command.

  7. Note down the number of IPv6 route tables in the standby... If it is less than the number noted in Step 2, wait for a few minutes and reverify until it reaches the number noted in Step 2.

  8. Issue ISSU run version from RP0 (active).

- CSCtx67028

  Symptom: Tracebacks are seen during a traffic condition when DMVPN and WAAS Express are configured.

  Conditions: This symptom is observed while initiating an FTP session from the GW, where GW DMVPN and WAAS Express are configured.

  Workaround: There is no workaround.

- CSCtx68155

  Symptom: Event is triggered as soon as configured and the **show event manager policy registered event-type timer-absolute** commad shows the wrong time value.

Conditions: Epoch-to-UNIX time conversion overflows after GMT: Thu, 07 Feb 2036 06:28:14. Also the timer_spec value passed to the timer is incorrect.

Workaround: Input of epoch value is limited to 2085978494(GMT: Thu, 07 Feb 2036 06:28:14) value assigned to timer_spec value is corrected.

- CSCtx74051

  Symptom: While performing an ISSU downgrade, IPv6 flexible netflow monitors may be displayed. Also, the running configuration is shown with incorrect subtraffic types.

  Conditions: This issue occurs during a downgrade to Cisco IOS Release 15.2(1)S (Cisco IOS XE Release 3.5). The monitors that are affected are those applied to IPv6.

  Workaround: The Netflow code should capture packets, as expected, on Cisco IOS Release 15.2(1)S. However, a reboot of the device should be performed before saving the running configuration because the affected configuration that is saved will be incorrect and will therefore fail to work at startup.

- CSCtx75190

  Symptom: In a multihomed setup, set up the traffic as explained in the DDTS. When the end-to-end traffic starts to flow smoothly, perform an RP switchover on ED1. Traffic from Ixia 3 to Ixia 1 and Ixia 3 to Ixia 2 on odd VLANs (ED1 is the AED for odd VLANs) is dropped with UnconfiguredMplsFia counters incrementing.

  Conditions: This symptom is observed when you perform an RP switchover with a scaled OTV configuration in a multihomed setup.

  Workaround: There is no workaround.

- CSCtx80535

  Symptom: The DHCP pool that is configured for ODAP assigns the same IP address to multiple sessions.

  Conditions: PPP users receive pool via Radius server. The pool is defined on the Cisco 10000 Series Routers to use the ODAP. The ODAP receives the subnets from the Radius server correctly, and assigns IPs to PPP sessions. However, sometimes, two users end up having the same IP address.

  Workaround: Clear the two sessions sharing the same IP address.

- CSCtx81562

  Symptom: LBM gets dropped when validated the replied data activated on ASR1000

  Conditions: This is seen when LBM is initiated with the validation flag.

  Workaround: The issue has been fixed in CSCtx81562. However, even without the fix, the CFM loopback can work without turning on the validation option as the workaround.

- CSCtx81748

  Symptoms: The occurance of a small amount of packet drops due to antireplay failure may be seen when IPSec is configured.

  Conditions: The packet drops may be seen either when the IPsec session brought-up or when the lifetime of IPSec SA expires and a new SA is established

  Workaround: There is no workaround.

- CSCtx82538

  Symptom: This DDTS has been raised to remove platform-specific macros.

Conditions: Platform specific macros are observed with CPU-specific checks. CPU-specific checks should not be in PI code. Use of shims is required.

Workaround: Remove CPU-specific checks.

- CSCtx86160

  Symptom: The following message appears when the **show interfaces** command is used when a SPA is being installed: `Hardware is N/A.`

  Conditions: This is seen on Cisco ASR1006 routers with12.2(33)XNF2c.

  In some scenarios of SPA hardware insert or removal combined with RP switchover, the hardware type string of interface stays at N/A. In some scenarios this is observed on both the standby RP and the active RP.

  Workaround: If only the active RP shows this message, single switchover is enough to recover. If both the active RP and the standby RP show this message, a double switchover must be performed.

- CSCtx88467

  Symptom: Configuring CEM PW on T1 controller and unconfiguring them once they are up. Memory leak is observed.

  Conditions: If a CEM PW is up, only incremental memory leak will be observed @ dsensor_subblock_get_or_create.

  Workaround: There is no workaround.

- CSCtx90571

  Symptom: The following Traceback message is logged when you unconfgure a packet tracing:

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

  Conditions: Configure and unconfigure packet tracing.

  Workaround: There is no workaround.

- CSCtx92598

  Symptom: The router crashes due to a low-memory condition caused by memory fragmentation. The following error message appears:

  ```
  Feb 10 05:59:21.874: %SYS-2-MALLOCFAIL: Memory allocation of 2372 bytes failed from
  0x5E77FC9, alignment 8 Pool: Processor Free: 33888144 Cause: Memory fragmentation
  ```

  Conditions: The router (seen on ASR 1000 RP2) that crashes will be an ingress PE for MVPN V6 with highly scaled configuration. PIM signaling, PIM SSM and data MDTS must be used in the core. Example scaling numbers are 600 mvrfs and 16 data mdts, 100 routers per mvrf;

  Note This issue will not occur if c-router signaling is used instead of PIM. The crash may occur in about 12 hours of running with the above configurations in a Cisco ASR1000 RP2 with typical memory size of 2 GB or 4 GB.

  Workaround: Perform one of these tasks:

  - Use smaller scaling numbers (much less than 600 movers, or 100 routes per mfr. or 16 data mdse. per mfr. in core)
  - Use c-route signaling in the core. A large amount of PIM control frames in the core can be avoided by using c-route signaling instead of PIM signaling.

  - Do not use data MDT; rely only on default. This also reduces the amount of PIM control frames that arrive at the ingress PE having a larger memory (say 4GB) will not help avoid the issue; the crash may happen after a longer duration.

- CSCtx94353

  Symptom: The following error message is displayed:

  ```
  %TUN-3-TUN_HA: Tunnel HA: Tunnel creation on standby: mismatching
  %COMMON_FIB-3-FIBHWIDBINCONS: An internal software error occurred. Tunnel0 linked to
  wrong hwidb Tunnel0
  ```

  Conditions: Create auto-tunnel number range with overlap with dynamic tunnels by other features such as multicast-routing.

  Workaround: Avoid usingan overlapping auto-tunnel number range with the other features.

- CSCtx97131

  Symptom: To send a VSA in an authentication and accounting request, the following commands have to be enabled:

  - **Router(config)#radius-server vsa send authentication**
  - **Router(config)#radius-server vsa send accounting**

  With the DDTS, these commands are enabled by default. The VSA will then send the corresponding authentication and accounting request.

  Conditions: `Router#sh run ? aaa Show AAA configurations l l Configuration with defaults ---- Router#sh run all | i radius-server  ........ radius-server vsa send accounting radius-server vsa send authentication.`

  Workaround: There is no workaround.

- CSCtx97298

  Symptom: The unsupported command **show ip accounting** is still available.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: Explicitly include or exclude command chains.

- CSCty01237

  Symptom: The following error message appears:

  ```
  %OER_BR-5-NOTICE: Prefix Learning STARTED CMD: 'show run' <timestamp>
  ```

  Conditions: This issue is seen under the following conditions:

  - If you configure PfR with a learn list, using a prefix list as a filter and enable learn.
  - If you use a configuration tool, script, or NMS that periodically executes the **show run**<*noCmdBold*> on the MC over HTTP or through some other means.

  Workaround: The following are the workarounds:

  - If you use the PFR Learn List feature, do not execute the **show run** command periodically.
  - If you use a monitoring tool that executes the **show run** command periodically, avoid using a learn list configuration in PfR.

- CSCty03745

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

Conditions: This symptom occurs when the IPv4 default route exists, for example, **ip route** *0.0.253.0 255.255.255.0 <next-hop>*.

Workaround: The following are the workarounds:

- Configure the next-hop-self for the BGP neighbors under the L2VPN VPLS address family, for example, **router bgp** *65000* **address-family l2vpn vpls neighbor** *10.10.10.10* **next-hop-self**
- Remove the default route or the static or IGP route from the IPv4 routing table.

- CSCty05282

  Symptom: The last reload reason in the **show version** command output is seen as `LocalSoft` after some reloads.

  Conditions: The conditions under which these symptoms are observed is unknown.

  Workaround: There is no workaround.

- CSCty05092

  Symptom: The EIGRP advertises the connected route of an interface that is shut down.

  Conditions: This is observed under the following conditions:

  - When you configure the EIGRP on an interface.
  - Configure an IP address with a supernet mask on the above interface.
  - Shut the interface. You will find that EIGRP still advertises the connected route of the above interface that is shut down.

  Workaround: The following are the workarounds:

  - Remove and add the INTERFACE VLAN xx.
  - Clear ip eigrp topology x.x.x.x/y.

- CSCty10285

  Symptom: WCCP redirection does not take place on a Cisco ASR 1000 Series Aggregation Services Router running Cisco IOS XE Release 3.5 RP1.

  Conditions: This symptom occurs when GetVPN is used.

  Workaround: There is no workaround.

- CSCty10635

  Symptom: The primary pseudowire is initially down in a PPP over L2TPv3 xConnect configuration with one or more backup pseudowires configured (pseudowire redundancy) and one of the backup pseudowires is up. The primary pseudowire eventually comes up after a delay of about 30 seconds.

  Conditions: This symptom is observed in PPP over L2TPv3 xConnect configurations with one or more backup pseudowires configured.

  Workaround: Configure a backup delay of 30 seconds or more to give the primary pseudowire a chance to come up before the backup pseudowire.

- CSCty12312

  Symptom: Multilink member links move to an Up or Down state and remain in this condition.

  Conditions: This symptom occurs after multilink traffic stops flowing.

  Workaround: Remove and restore the multilink configuration.

- CSCty12524

Symptom: The BRI packet from the LMA is not handled properly on the MAG. Also the MAG is not sending the APN and SSMO option in PBRA.

Conditions: This symptom is observed on the originating or old MAG while clearing sessions in LMA in response to the mobile node roaming to a new MAG.

Workaround: There is no workaround.

- CSCty15471

  Symptom: Sometimes, the primary pseudowire comes as standby while secondary becomes up.

  Conditions: This occurs only with 'backup never' in the redundancy configuration. Also, it is a timing issue and does not occur always and depends on when the primary and secondary PWs are coming up.

  Workaround: Perform a manual switchover to primary.

- CSCty19713

  Symptoms: The ESP or CPP of a Cisco ASR 1000 Series Aggregation Services Router crashes.

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

  Workaround: There is no workaround.

- CSCty21156

  Symptom: Incorrect states are displayed in the MRIB/MFIB tables when the IGP and the BGP are removed from the setup.

  Conditions: On removing the IGP and BGP configurations on a PE router, the MRIB states in the core get messed up.

  Workaround: Unconfigure the VRF before removing the IGP andBGP or clear the mroute states.

- CSCty25093

  Symptom: The BDI option is missing under the **show standby** command.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: Collect BDI-specific data using the **show standby** command.

- CSCty28813

  Symptom: When VRFa's mdt_default address is configured to VRFb's mdt_data group address, the router will end up crashing or CPU hog.

  Conditions: When VRFa's mdt_default address is configured of address of other MVRF, this condition occurs.

  Workaround: Have to manually check whether the address of mdt_default has already been used before.

- CSCty29122

  Symptom: TCP TLS handshake fails for secure RTP calls.

  Conditions: The symptom is observed with Cisco IOS interim Release 15.2(03.1)T.

  Workaround: There is no workaround.

- CSCty31373

  Symptom: The fman_fp logs get filled with messages that are not helpful.

  Conditions: The DVTI hub on ASR1000 router

Workaround: There is no workaround.

- CSCty34896

  Symptom: Synchronization fails while setting **entPhysicalAlias** through the SNMP for the following MIB entities: RP A Internal Bootflash RP A flash card 0 SFP 7/1/0/0 module 1/1", DESCR: "2 port DTI UC" -> 2 DTI cards

  Conditions: This issue occurs on a Cisco uBR10012 Router.

  Workaround: Do not set **entPhysicalAlias** for these MIB entries.

- CSCty37233

  Symptom: A Layer 3 (routed) interface can be converted to a Layer 2 (switched) interface by applying the switchport configuration command. If the interface was configured as a VNET trunk, the VNET subinterfaces are deleted. Subsequently, if the switchport command is removed, the VNET trunk configuration will reappear, but the VNET trunk will no longer be functional. When a switchover is performed following the sequence above, the new active takes over as expected, but when the old active reboots as the standby, configuration synchronization fails because the standby attempts to create the VNET subinterfaces that no longer exist on the active. This results in an ifindex-sync failure and a PRC error that causes the RP to go into a continuous reboot loop.

  Conditions: The reboot problem will occur only on switch platforms with a redundant RP.

  Workaround: Remove the VNET trunk configuration from an interface before converting it from Layer 3 to Layer 2.

- CSCty37836

  Symptom: The ceqfpMemoryResourceTable does not include DRAM values.

  Conditions: This issue occurs when the **ceqfpMemoryResourceTable** is queried.

  Workaround: There is no workaround.

- CSCty41336

  Symptom: Forward-alarm AIS does not work on the CESoPSN circuits.

  Conditions: This symptom occurs when you create SAToP and CESoPSN circuits and configure forward-alarm AIS.

  Workaround: There is no workaround.

- CSCty41692

  Symptom: The standby PRE crashes while the IPV4 VRF AF is added on the active PRE. No issues are seen with the active PRE.

  Conditions: This occurs only when unconfiguration and reconfiguration is done when the BGP is in read-only mode.

  Workaround: After the BGP exits the read-only mode, this issue does not occur.

- CSCty42453

  Symptom: All pending acknowledgmentare seen on the ATM interface.

  Conditions: This issue is seen during OIR reloads.

  Workaround: There is no workaround.

- CSCty44654

  Symptom: Router Crashes when trying to test the MVPN6 functionality.

Conditions: The following are the conditions:

- Configure the router to test the MVPN6 functionality.
- Delete the VRF associated with the interface in the MVPN6 test configuration.
- The router crashes.

Workaround: There is no workaround.

- CSCty47491

  Symptom: Differences are observed in **show mpls ldp igp sync all** command output. This behavior is seen across all the platform while testing the mcp_dev build.

  Conditions: This symptom is observed during both manual and automated testing of mcp_dev build.

  Workaround: There is no workaround.

- CSCty48870

  Symptom: Router crash due to a bus error.

  Conditions: This has been observed in a router that is running Cisco IOS Release 15.2(2)T and Release 15.2(3)T with the NBAR enabled on a crypto-enabled interface. The NBAR can be enabled through NAT, QoS, or NBAR protocol discovery.

  Workaround: Using the **no ip nat service nbar** command will help where NBAR is enabled through NAT.

- CSCty51082

  Symptom: The LPD Group Trap is not sent on a connection loss.

  Conditions: On connection loss, LDP Group Trap should be sent.

  Workaround: If you have **auto ip sla mpls-lsp-monitor reaction-configuration 100 react lpd lpd-group retry 3** configured in addition to the **auto ip sla mpls-lsp-monitor reaction-configuration 57 react lpd tree-trace action-type trapOnly** command.

- CSCty55408

  Symptom: All pending issues and acknowledgments are observed after unconfiguring and then reconfiguring the same-scale configurations while traffic is running.

  Conditions: configure 4 overlays with 500 EFPs per overlay set up the traffic as described in the DDTS start traffic. Remove the overlay and EFP config copy the same config back on one of the otv routers.

  Workaround: There is no workaround.

- CSCty55449

  Symptom: The device crashes after registering an Embedded Event Manager TCL policy.

  Conditions: If the policy uses the Multiple Event feature and the trigger portion is registered without curly braces ({}), the device will crash.

  Workaround: Make sure that the trigger portion that is the correlate statement, is enclosed within curly braces.

- CSCty56850

  Symptom: Routers are not updating the cnpdAllStatsTable with traffic from all the expected protocols.

  Conditions: This symptom is observed with routers that are running Cisco IOS 15.x (tested in Release 15.0, 15.1 and Release 15.2(2)T).

Workaround: Perform one of these tasks:

- Usethe **show IP NBAR protocol-discovery** command to get the statistics for all the protocols.
- Perform a **snmpget** against the objects inthe cnpdAllStats table.

- CSCty64255

  Symptom: BGP L3VPN dynamic route leaking feature from the VRF to global export feature, the prefix limit is incorrect upon soft clear, or new prefix added, or prefix deleted.

  Conditions: This symptom is observed when VRF to global export is enabled, and prefix limit is configured.

  Workaround: BGP hard clear.

- CSCty65226

  Symptom: Memory leak is observed in Cisco ASR1000 Series Aggregated Services Routers.

  Conditions: This issue is seen when multiple service instances are configured and unconfigured.

  Workaround: There is no workaround.

- CSCty66799

  Symptom: The standby RP reloads and the BOOT parameter in the boot loader is lost.

  Conditions: When we have a candidate default static route that is learned from a DHCP server on an active router and while issuing the **no ip route*** command.

  Workaround: There is no workaround other than not issuing the **no ip route*** command.

- CSCty68402

  Symptom: NTT model 4 configurations are not taking effect.

  Conditions: None

  Workaround: There is no workaround.

- CSCty69946

  Symptom: When the port channel with many subinterfaces is deleted and the **show run** command is run on the member links, the member links are still associated with the port channel. After the port channel is reconfigured, it does not come up.

  Conditions: This issue is seen when a port channel with many subinterfaces is deleted.

  Workaround: Reconfigure the **channel-group x** command on the member link.

- CSCty71843

  Symptom: Tracebacks are observed in the **lfd_sm_start** and **lfd_sm_handle_event_state_stopped** APIs during router bootup.

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

  Workaround: There is no workaround.

- CSCty73817

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

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

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

- There are a large amount of sessions.
- The QoS Policy Accounting feature is used.
- Switchover is performed.

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

- CSCty74859

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

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

  Workaround: There is no workaround.

- CSCty76106

  Symptom: Crash occurs after two days of soaking with traffic.

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

  Workaround: There is no workaround.

- CSCty76180

  Symptom: The XConnect entries get deleted and stay down.

  Conditions: This issue occurs while configuring CEM groups and performing a switchover.

  Workaround: There is no workaround.

- CSCty77441

  Symptom: Memory leak is seen while unconfiguring BFD sessions.

  Conditions: This issue is seen while unconfiguring BFD sessions.

  Workaround: There is no workaround.

- CSCty78435

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

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

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

- CSCty80691

  Symptom: Traceback is seen from the DFC linecard.

  Conditions: Reload the router with the scale of the configuration.

  Workaround: There is no workaround.

- CSCty83996

Symptoms: Prior to a switchover, CoA a service logon session is present in both the active RP and the standby RP. After the switchover, CoA service logon is executed and then the session is positoned on the standby RP.

Conditions: The issue occurs after the switchover, when CoA service logon is executed.

Workaround: There is no workaround.

- CSCty85918

  Symptom: WRED on PPPoE session does not match on DSCP/PREC with MPLS traffic.

  Conditions: PPPoE get terminated on a Cisco ASR1000 Series Aggregation Services Router acting as LNS. The L2TP circuit is actually MPLS switched out of the router. The policy map correctly matches packets into the corresponding class, but WRED always has the packets matching the WRED default class. The packets should match a DSCP or PREC value because the policy map is on the session and not on the egress physical interface.

  Workaround: If MPLS is removed from the egress L2TP tunnel interface, the packets are classified correctly by WRED.

- CSCty85926

  Symptom: VC (VPLS/EoMPLS) will stay down with the following message when the **show mpls l2 vc detail** command is used:

  ```
  Signaling protocol: LDP, peer unknown
  ```

  Conditions: This symptom will occur if you have LDP GR configured. Perform an SSO switchover and try configuring the VC after the switchover is complete.

  Workaround: There is no workaround. Reload the switch.

- CSCty86039

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

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

  Workaround: There is no workaround.

- CSCty86146

  Symptom: Sometimes, the ISIS attached bit is not updated when the area address is changed.

  Conditions: When the area address is changed, if there is no adjacency, the state is changed.

  Workaround: Run the **clear isis *** command.

- CSCty86543

  Symptom: The following error message must be displayed under heavy IPv6 traffic load on the IPSec SVTI router :

  ```
  %IOSXE-3-PLATFORM: SIP0: cpp_cp: QFP:0.0 Thread:006 TS:00000002120506574235
  %IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 37     *Mar 23
  16:06:11.329: %IOSXE-3-PLATFORM: SIP0: cpp_cp: QFP:0.0 Thread:108
  TS:00000002194684194075 %IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error,
  DP Handle 11  *
  ```

  Conditions: Send the IPv6 traffic to the Kingpin router from the peer router side at 10G port line rate with a frame size of 64 bytes.

  Workaround: There is no workaround.

- CSCty88146

  Symptom: This is a development bug to improve the efficiency of the RIB.

Conditions: This symptom is not caused by any specific condition.

Workaround: There is no workaround.

- CSCty89224

  Symptom: A Cisco IOS router crashes under certain circumstances while receiving an MVPN v6 update.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: There is no workaround.

- CSCty89777

  Symptom: The committed Memory value of 96 percent exceeds the critical level of 95 percent messages on the router console with a 4G CCN image.

  Conditions: On a 16G router, IOSD gets 11G, leaving 5G to virtual instance and other Linux processes. 16G is enough for real physical memory usage but smand is pretty conservative and it counts virtual memory or allocated memory, which is different from the actually committed physical memory. 3PA is added, that is, QEMU/CCN and 4G memory is preallocated and passed into the guest regardless of whether the guest actually uses all of that memory. In such a situation, in this situation where the virtual memory is large, but the real memory that is in use could actually be way smaller.

  Workaround: There is no workaround.

- CSCty91465

  Symptom: The VRF interface does not work even if the policy maps are configured correctly to receive the packets from the VRF interface.

  Conditions: The symptom is observed when CEF is enabled.

  Workaround: Disable CEF.

- CSCty96049

  Symptom: Cisco IOS software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Condition: An attacker could exploit this vulnerability by sending a single DHCP packet or through an affected device, causing the device to reload.

  Workaround: Cisco has released free software updates that address this vulnerability. The advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp. 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.

- CSCty96052

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

  Conditions: This is an extreme corner case or timing issue. It has been observed only once on the release image.

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

- CSCty97784

  Symptom: The router crashes.

Conditions: This symptom is observed when NBAR is enabled, that is, match protocol actions in the QoS configuration or IP NBAR protocol discovery on an interface or NAT is enabled, and IP NAT service NBAR has not been disabled.

Workaround: There is no workaround.

- CSCtz00431

  Symptom: The device crashes and tracebacks are seen in the syslog process.

  Conditions: This symptom is observed with the following procedure:

  1. Configure a capture point and start it.

  2. Remove the policy map associated with the capture point. It throws an error the first time but accepts it the second time.

  3. Stop the capture point.

  4. Restart the capture point.

  Workaround: Do not remove the policy map associated with the capture point while the capture is active.

- CSCtz02097

  Symptom: When configuring HSRP on a port channel, the following warning message is displayed if you try to configure over 28 HSRP groups on the port-channel:

  ```
  % Warning: Interface MAC address filter only supports 28 additional addresses  % and
  28 HSRP groups are already configured. The HSRP MAC address may not be  % added to
  the MAC address filter if the group becomes active.
  ```

  Condition: This issue occurs when configuring HSRP on a port channel

  Workaround: There is no workaround.

- CSCtz03779

  Symptom: The standby RSP crashes during ISSU.

  Conditions: This issue occurs Occurs when you perform an ISSU downgrade from Release 3.6 to Release 3.5.

  Workaround: There is no workaround.

- CSCtz04223

  Symptom: The interface virtual template <x> type tunnel can be configured from the CLI. This command should be removed from the CLI because it is unsupported.

  Conditions: Cisco Catalyst 7600 series running 15.2S

  Workaround: There is no workaround.

- CSCtz11265

  Symptom: The fman_rp type memory leak was seen during longevity testing for about 10 days

  Conditions: 16k bhca ppp flap and MLD Zap 3-play traffic 7 MIB macros Cmd_load macro ASR_So macro

  Workaround: There is no workaround.

- CSCtz12525

  Symptom: An accounting stop is sent without Acct-Input-Packets Acct-Output-Packets Acct-Input-Octets Acct-Output-Octets when service stop is performed.

  Conditions: This symptom is observed when service stop is performed for the prepaid service.

Workaround: There is no workaround.

- CSCtz13465

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

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

  Workaround: There is no workaround.

- CSCtz13818

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

  Conditions: This symptom is observed when a route map (export map) is configured under VRF and the route map is updated with a new route target. In this scenario, Cisco IOS software does not send refreshed updates with modified route targets.

  Workaround: The following are the workarounds:

  - Refresh the updated route target to use the **clear ip route vrf** <*vrf-name net mask*> command.
  - Clear the BGP session with the peer.

- CSCtz18966

  Symptom: The MDT tunnel does not come up in a particular sequence of events.

  Conditions: If BGP update source interface is deleted, added again, and the peer group is configured with the update source, the MDT tunnel does not come up.

  Workaround: It is uncommon to delete the update source loopback and add it back again. It is found through internal negative testing.

- CSCtz18992

  Symptom: The ... Router sends the EIGRP query even in the ... Router split horizon interface.

  Conditions: This problem is noticed when a router gets a query message immediately after sending an initial update to another router.

  Workaround: The issue does not have a visible impact. Hence, no workaround is required.

- CSCtz19080

  Symptom: The sending of "**rttMonCtrlOperTimeoutOccurred**" on Release 12.2(33)XNF and Release 12.4(15)T. results in "**rttMonCtrlOperOverThresholdOccurred**" getting sent in the latest Release 15.1. Also, the RTT falling threshold "**rttMonCtrlOperOverThresholdOccurred**" that is sent on Release 12.2(33)XNF results in "**rttMonCtrlOperVerifyErrorOccurred**" getting sent in the Release 15.1.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: There is no workaround.

- CSCtz21299

  Symptom: PfR MC may show some traffic classes are uncontrolled due to an exit mismatch.

  Conditions: This symptom is observed when PfR optimizes traffic class with PBR in a scale DMVPN setup, and when there is a brownout in one of the links.

  Workaround: There is no workaround.

- CSCtz21718

  Symptom: One-way latency measurements display spikes.

  Conditions: Enable "**precision timestamp**" and "**optimize timestamp**".

Workaround: Use normal timestamping instead of the "**optimize timestamp**" option.

- CSCtz22062

  Symptom: The extranet MVPN multicast receivers get intermittent duplicate and missing packets. The operations of one day showed about 10 duplicates/misses.

  Conditions: The issue is observed when the receivers are on remote PE routers and receive streams by means of the MDT tunnel. Local receivers on the same PE router are unaffected. In which setup, customers have a source VRF, a transport VRF, and receiver a VRF. The source is connected to C10K in the source VRF, and it was observed that this (ingress) C10K is responsible for the drops and duplicates.

  Workaround: There is no workaround.

- CSCtz22400

  Symptom: CPP timestamp with NAT, that has enabled "optimize timestamp" ip sla fails.

  Conditions: Config "optimize timestamp" for ip sla.

  Workaround: There is no workaround.

- CSCtz23433

  Symptom: ISG shell maps with a policer on the egress child default-class fail.

  Conditions: This symptom is seen in shell maps with a policer or a shaper on the child default-class.

  Workaround: There is no workaround.

- CSCtz23514

  Symptom: An FMAN-FP crash is caused by memory corruption.

  Conditions: This issue occurs whenthe BBA session login and logout is in high scaling, and the LI tap is enabled on some sessions.

  Workaround: There is no workaround.

- CSCtz23638

  Symptom: The following error message is displayed on the console:

  ```
  PLIM driver informational error txnpTooLittleData
  ```

  Conditions: The issue occurs when the SIP40 carrier card is present in the router along with any of the following SPAs: SPA-1CHOC3-CE-ATM SPA-1XCHOC12/DS0 SPA-1XCHSTM1/OC3 SPA-1XCHSTM1/OC3W (This is the same SPA as SPA-1XCHSTM1/OC3 that is included in "SB" bundles - special pricing) SPA-24CHT1-CE-ATM * SPA-2CHT3-CE-ATM SPA-2X1GE-SYNCE SPA-2XCT3/DS0 SPA-2XT3/E3 SPA-4XCT3/DS0 SPA-4XCT3/DS0-WE (This is the same SPA as SPA-4XCT3/DS0 that is inccluded in the SB bundles - special pricing) SPA-4XT3/E3 SPA-8XCHT1/E1 SPA-DSP SPA-WMA-K9.

  Workaround: There is no workaround.

- CSCtz24454

  Symptoms: POS interfaces are stuck in the down state.

  Conditions: This symptom is observed on the router reload/ SPA reload.

  Workaround: Perform an FP reload to bring the interfaces back up.

- CSCtz25825

  Sympton: Null0 route for summary remains even if aggregate-address is removed from all the VRFs.

  Conditions: The issue occured when a connected route is imported from a different VRF, and the same aggregate-address command is configured in each VRF.

Workaround: There is no workaround.

- CSCtz25953

  Symptom: The following error message is displayed, and certain length packets get dropped:

  ```
  LFD CORRUPT PKT
  ```

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

  Workaround: There is no workaround.

- CSCtz26188

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

  Conditions: This symptom occurs if the configured value of the cleanup timer is 60 seconds. then Packets may be lost on platforms in which the forwarding updates take longer.

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

- CSCtz26580

  Symptom: After enabling the "**debug platform hardware qfp active feature ipsec datapath trace**" command on a Cisco ASR1000 Series Aggregation Server Routers acting as GET VPN GM, if a fragmented UDP packet comes through the IPsec tunnel, and the last IP fragment is 36 bytes or less (20 header 1 to 16 payload), the packet is dropped with the message `PacketProcessingExcept[ions],` and `%INFRA-3-INVALID_GPM_ACCESS is logge`d.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: Disable the debug.

- CSCtz26683

  Symptom: An unsupported IP verify unicast ... configuration applied to an interface may still be shown in **show running-config** after being rejected. Output similar to the following will appear when applying the configuration:

  ```
  % ip verify configuration not supported on interface Tu100   - verification not supported by hardware % ip verify configuration not supported on interface Tu100   - verification not supported by hardware %Restoring the original configuration failed on Tunnel100 - Interface Support Failure
  ```

  Conditions: This symptom occurs when there is no prior IP verify unicast ... configuration on the interface and when the interface or platform or both do not support the given RPF configuration.

  Workaround: In some cases, it may be possible to get back to the previous configuration by using the **no** form of the command. In other cases, reload the device without saving the configuration, or edit the configuration manually if already saved.

- CSCtz26658

  Symptom: A Cisco ASR 1000 Series Seggregation Services Router acts as GET VPN GM. Small UDP fragments (21 to 25 bytes, including IP header) that come in through IPsec are dropped.

  Conditions: This symptom occurs when a Cisco ASR 1000 Series Aggregation Services Router acts as GET VPN GM and TBAR is enabled for the group.

  Workaround: There is no workaround.

- CSCtz28544

Symptom: The Cisco ASR 1000 Series Aggregation Services Routers that are configured for Multicast Listener Discovery (MLD) tracking for IPv6 may reload after receiving certain MLD packets. The following traceback will be shown in the logs:

```
Exception to IOS Thread: Frame pointer 4081B7D8, PC = 1446A878 ASR1000-EXT-SIGNAL:
U_SIGSEGV(11), Process = MLD
```

Conditions:This issue occurs in the Cisco ASR 1000 Series Aggregation Services Routers that are configured for MLD tracking for IPv6.

Workaround: The only workaround is to disable MLD tracking. PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores at of the time of evaluation were 6.1/5.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C CVE ID CVE-2012-1366 has been assigned to document this issue.

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

- CSCtz31217

  Symptom: The DNS portion of the HTTP command does not use the configured source IP.

  Conditions: This symptom occures when the HTTP operation is configured with source IP and host name instead of the IP address of HTTP server (which will require a DNS lookup).

  Workaround: There is no workaround.

- CSCtz31420

  Symptom: EIGRP delay calculation is broken and an unknown delay is shown.

  Condition: The issue can be shown on 15.1(3)S2 (3.4.2S).

  Workaround: There is no workaround.

- CSCtz31972

  Symptom: The Rcvd in Used as bestpath does not count up in show ip bgp neighbor as follows:

```
R511#sh ip bgp nei 10.1.1.2    BGP neighbor is 10.1.1.2,  remote AS 200, external link
(snip)                                  Sent       Rcvd    Prefix activity:
----      ----     Prefixes Current:           1        1     Prefixes Total:
1         1     Implicit Withdraw:           0         0     Explicit Withdraw:
0           0      Used as bestpath:             n/a           0 <--no count-up
R511#sh ip bgp nei 10.1.1.2 route  (snip)    *>  20.2.2.0/24    10.1.1.2    0     0 200 i
```

  Conditions: This symptom is observed in 15.2(3)T.

  Workaround: There is no workaround.

- CSCtz32360

  Symptom: After bootup or initial interface configuration, a Cisco ASR1002 Router with Sync-E SPA may indicate an interface and a QL-PRC network clock state although no cable is connected and no valid clock is received on that interface. In addition, when there is a valid clock, the LED may continue to display amber.

  Conditions: This issue is observed primarily after booting a Cisco ASR 1002 Router , or when the interface is initially configured.

Workaround: A possible workaround is to unplug and replug the cable of the affected port. Alternatively, the affected port can be locked out with the **network-clock set lockout <port> 2048k** command when the clock is not fed to the port. After the clock is fed, the lockout can be cleared using the **network-clock clear lockout <port> 2048k** command.

- CSCtz35465

  Symptom: Banner and refuse message are similar implementations.

  Conditions: While nvgening, the refuse message should handle the \r character.

  Workaround: Handle the '\r ' character while nvgening.

- CSCtz37164

  Symptom: The requests to the RADIUS server are retransmitted even though the session no longer exists, causing unnecessary traffic to the RADIUS, and the RADIUS receiving requests for an invalid session.

  Conditions: This symptom occurs when the RADIUS server is unreachable and the CPE times out the session.

  Workaround: This is currently being worked upon. This issue can be avoided by making sure that the RADIUS server is always reachable.

- CSCtz37863

  Symptom: IPCP is not in an open state and does not call the This-Layer-Down (TLD) vector.

  Conditions: This symptom is observed if IPv4 saving is enabled and IPCP negotiation failed because of a TermReq received from peer.

  Workaround: There is no workaround.

- CSCtz38010

  Symptom: The platform maximum numbers for Cisco ASR1000 NAT44 and NAT64 are not set for KP and FP80.

  Conditions: This issue occurs when the scalability numbers are incorrect.

  Workaround: There is no workaround.

- CSCtz38558

  Symptom: A traceback may be seen on a Cisco ASR1000 Series Aggregation Router when processing some of the IPv6 malformed packets.

  Conditions: The issue occurs when an IPv6 packet is malformed.

  Workaround: There is no workaround.

- CSCtz38812

  Symptom: The **show ssh ?** command does not produce the complete output.

  Conditions: The issue occurs when the rekey is disabled.

  Workaround: There is no workaround.

- CSCtz40559

  Symptom: The incorrect flags in the IP Address duplicate check that prevents VRRP3 does not impact any usage currently. It is only applicable for future VRRP v3.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: There is no workaround.

- CSCtz40705

Symptom: A configuration change that results in a serial interface being unconfigured may cause the router to reload if the serial interface is a XConnect member.

Conditions: This symptom has been observed when the **xconnect** command is configured on a channelized T1 serial interface with HDLC encapsulation, andthe **no** *t1 channel channel-group channel-group-number* command is configured to remove the channel group.

Workaround: Remove the serial interface from the XConnect using the **no xconnect** command.

- CSCtz41046

  Symptom: Cisco devices that run Cisco IOS may experience a minor memory leak when malformed CDP packets are received. This could result in stability issues after extended periods of time under certain circumstances.

  Conditions: Cisco devices running an affected version of Cisco IOS.

  Workaround: Disable CDP packets on the affected device. In global configuration mode: **no cdp run**

  Further Problem Description: This issue was identified during an internal security audit of Cisco devices.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores at the time of evaluation were 3.3/3. https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:P/E:POC/RL:U/RC:C

  No CVE ID has been assigned to this issue.

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

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

- CSCtz41048

  Symptom: The **trace mpls ipv4** command is unsuccessful.

  Conditions: This symptom is observed when the **trace mpls ipv4** command is issued.

  Workaround: There is no workaround.

- CSCtz42336

  Symptom: Compilation error on upgrading compiler.

  Conditions: Upgrading ICC compiler 10.2 to 11.2.

  Workaround: Use ICC 10.2.

- CSCtz44141

  Symptom: An unexpected error message is seen when configuring the WCCP redirect-list ACL. For example:

  ```
  Router(config)#ip access-list extended wccp-acl Router(config-ext-nacl)#permit tcp any any gt 20 Router(config-ext-nacl)#exit Router(config)#ip wccp 100 redirect-list wccp-acl %warning, complex WCCP access-list: "port operator", sequence: 10
  ```

  Conditions: The issue occurs when the WCCP is configured with a redirect-list ACL.

  Workaround: There is no workaround. Ignore the error message.

- CSCtz44363

  Symptom: The following Emitting error message is displayed multiple times for each class when the **show policy-map int** command is executed:

```
Port-channel2 has more than one active member link.
```

Conditions: This issue occurs under any of the following conditions:

1. The **lac max-bundle 1** command is not configured on Port-Channel interface.

2. This case is applicable to uut as LNS in QoS PPPoGEC.

Workaround: Ensure that the **lac max-bundle 1** command is configured for the port channel interface.

- CSCtz44625

  Symptom: Deconfigure import ipv4 unicast map incorrectly removes the import ipv4 multicast map under VRF, and vice versa. The same holds for the export ipv4|ipv6 unicast|multicast map command.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: Reconfigure the incorrectly deleted command.

- CSCtz44989

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

  Conditions: This issue is seen in IPv6 link-local nexthop. When the EIGRP route is redistributed to BGP VRF, it clears the nexthop information (it becomes 0.0.0.0). Subsequently, Now this route becomes invalid and BGP cannot export to another VRF.

  Workaround: There is no workaround.

- CSCtz45901

  Symptom: The output of the **show run** or the **format xml** command for an ATM interface is not displayed in the correct order.

  Conditions: This symptom is observed if there are multiple subinterfaces for an ATM interface and PVC is configured under these.

  Workaround: There is no workaround.

- CSCtz46305

  Symptom: Unable to poll eigrp mib.

  Conditions: On ASR 1000 - 3.6.0 15.2(2)S

  Workaround: There is no workaround.

- CSCtz48338

  Symptom: A router may crash with setup with configuration of BGP L3VPN VRF to global export, NSR, and large scale, hard clear or link flap.

  Conditions: This symptom is seen under the following conditions:

  - BGP L3VPN VRF to global import
  - NSR
  - Large scale

  Workaround: There is no workaround.

- CSCtz49471

  Symptom: The LSP trace route does not indicate midpoint labels.

  Conditions: This issue is seen over static MSPW segments.

  Workaround: There is no workaround.

- CSCtz49578

  Symptom: MPLS TP link-management admission failures are seen on the midpoint node, causing LSP programming failure.

  Conditions: This issue is seen intermittently during Cisco ASR903 on reload.

  Workaround: Remove and reattaching the configuration.

- CSCtz50683

  Symptom: When 10 x MDLP sessions are removed, one or more hardware adj remains. This occurs due to incorrect removal of LSPs.

  Conditions: This symptom is observed when more than eight sub-LSPs occur.

  Workaround: Do not use more than eight sub-LSPs.

- CSCtz51081

  Symptom: Attempts to configure the SNMP-SERVER HOST for EIGRP results in the EIGRP line changes to VDSL2LINE. `C2921(config)#snmp-server enable traps eigrp C2921(config)#exit C2921#show Apr 24 23:03:54.031: %SYS-5-CONFIG_I: Configured from console by co C2921# C2921# C2921#show run | i snmp snmp-server community cisco RW snmp-server enable traps eigrp C2921#conf t Enter configuration commands, one per line. End with CNTL/Z. C2921(config)#snmp-server host 10.0.0.1 traps version 2c NETMANAGER eigrp C2921(config)#exit C2921#show run | i snmp snmp-server community cisco RW snmp-server enable traps eigrp snmp-server host 10.0.0.1 version 2c NETMANAGER vdsl2line`

  Conditions: Cisco2921 with 15.1.4(M4). Other versions may be affected.

  Workaround: There is no workaround.

- CSCtz51719

  Symptom: SA warnings in ipmulticast component code.

  Conditions: SA warnings in ipmulticast component code in rc_texel.

  Workaround: Fixed.

  Further Problem Description: SA warnings.

- CSCtz51846

  Symptom: Packets are not routed through the expected interface.

  Conditions: This issue occurs when you configure access lists and create PBR to route packets by means of different DVTIs to match different access group.

  Workaround: There is no workaround.

- CSCtz52025

  Symptom: Tracebacks are seen with 30K ACE HA.

  Conditions: This occurs during FP reload and RP reload.

  Workaround: There is no workaround.

- CSCtz53335

  Symptom: In show-run, sequence interval is displayed next to policy map instead of in the next line.

  Conditions: When applying sequence-interval command on a policy-map, show run should display sequence interval at the next line after policy-map name, but it incorrectly displays the commands next to policy-map.

Workaround: There is no workaround.

- CSCtz53398

  Symptom: A ping sweep from ASR1000 with size 11871 - 18024 fails.

  Conditions: `ASR#ping Protocol [ip]: Target IP address: 10.222.202.49 Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y Source address or interface: Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: y Sweep min size [36]: 11871 Sweep max size [18024]: Sweep interval [1]: Type escape sequence to abort. Sending 30770, [11871..18024]-byte ICMP Echos to 10.222.202.49, timeout is 2 seconds: !!.....!.....!.....!.....!..... .... Success rate is 3 percent (6/178), round-trip min/avg/max = 1/1/2 ms asr1002-x#sh ip traffic IP statistics: Rcvd: 186570321 total, 222 local destination 0 format errors, 0 checksum errors, 0 bad hop count 0 unknown protocol, 0 not a gateway 0 security failures, 0 bad options, 0 with options Opts: 0 end, 0 nop, 0 basic security, 0 loose source route 0 timestamp, 0 extended security, 0 record route 0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump 0 other, 0 ignored Frags: 61 reassembled, 42 timeouts, 0 couldn't reassemble 61 fragmented, 122 fragments, 0 couldn't fragment Bcast: 198 received, 0 sent Mcast: 14 received, 29 sent Sent: 52 generated, 44723000 forwarded Drop: 0 encapsulation failed, 0 unresolved, 0 no adjacency 0 no route, 0 unicast RPF, 0 forced drop, 0 unsupported-addr 0 options denied, 0 source IP address zero There was no issue seen if the same ping test was issued from the GSR router. The ping to the ASR1k itself also fails: ------------------------ ASR#sh ip int br Interface IP-Address OK? Method Status Protocol Te0/0/0 10.222.202.50 YES manual up up ASR#ping 10.222.202.50 size 11873 repeat 10 Type escape sequence to abort. Sending 10, 11873-byte ICMP Echos to 10.222.202.50, timeout is 2 seconds: .... Success rate is 0 percent (0/10) ASR#`

  Workaround: There is no workaround.

- CSCtz54207

  Symptom: After the master stack is down, net hop address is duplicated on "ip next-hop".
  `---------- 3750X#sh rout route-map TEST, permit, sequence 10 Match clauses: ip address (access-lists): PBR Set clauses: ip next-hop 192.168.1.254 192.168.1.254 <<< Policy routing matches: 0 packets, 0 bytes ----------`

  Conditions: configure route-map. `3750X(config)#no route-map TEST 3750X(config)#route-map TEST 3750X(config-route-map)#ma ip add PBR 3750X(config-route-map)#set ip next 3750X(config-route-map)#set ip next-hop 192.168.1.254`

  Workaround: There is no workaround.

- CSCtz54338

  Symptom: The Valgrind tool reports a memory issue in fman_acl_bind_ack_cb().

  Conditions: This issue is seen after run valgrind tool is run.

  Workaround: There is no workaround.

- CSCtz54535

  Symptom: OTV packets are dropped for 1 minute when the ED gets back to AED from the No ISIS neighbor at Join-interface status.

  Conditions: The issue occurs under normal conditions

  Workaround: There is no workaround.

- CSCtz55138

  Symptom: The "**snmp-server enable traps ISG-MIB**" commnd is not shown in the running configuration.

  Conditions: This issue does not occur under a specific conditions.

  Workaround: There is no workaround.

  Further Problem Description: The "**snmp-server enable traps ISG-MIB**" command is not getting nvgen. Therefore, a trap can neither be enabled or disabled from CLI.

- CSCtz55297

  Symptom: Credit allocation is not changed when sessions are changed from unauthenticated to authenticated.

  Conditions: The existing nonauthenticated session needs to be modified to authenticated session.

  Workaround: There is no workaround.

- CSCtz55363

  Symptom: In the Cisco ASR Series Aggregation Routers, changing the speed on the main interface does not change the Delay (DLY) value for the earlier configured subinterfaces.

  Conditions: This issue occurs when the subinterfaces configured.

  Workaround: 1.)Reload the router. 2.)Reconfigure the subinterface.

- CSCtz55923

  Symptom: The TTL field of the IPv4 header is reset after routing through ASR1000 after reloading the router.

  Conditions: NAT configuration along with '**no ip nat service dns-reset-ttl**'.

  Workaround: Remove and readd the **no ip nat service dns-reset-ttl** command configuration after reloading the Cisco ASR1000 Series Aggregation Services Router after all the cards are in an 'OK' state.

- CSCtz55969

  Symptom: Changes to a custom profile are reflected in the actual packet transmission rates.

  Conditions: Video with a custom profile

  Workaround: Remove the corresponding profile, and create a new one with the required changes.

- CSCtz56671

  Symptom: An ACL is applied for filtering within a classmap for shaping traffic. When you try to resequence the ACL, the class map DB is not populated with new sequencing, and that causes a crash.

  Conditions: ACL resequence that should be used within class-map

  Workaround: Do not use resequencing, or remove and re-add the same after resequencing.

Further Problem Description: **ip access-list resequence <ACL #/name>** followed by either a **no <ACE #>** or a **no <ACL #/name>**. The crash occurs inside the MDB and the root cause of this crash is that the sequence numbers stored in the MDB are out of sync with the sequence numbers stored in ACL. Therefore, when the **no ACE #** command is issued, the MDB tries to delete that ACE from its tree, but never finds it and gets stuck in a loop.

- CSCtz58037

  Symptom: The router crashes after **Shut no shut** and OIR commands.

  Conditions: The issue occurs when the router is configured with the **cfm one up mep** command and the **cfm down mep** command with trunk EFP.

  Workaround: There is no workaround.

- CSCtz58941

  Symptom: The router crashes when users execute the show ip route XXXX<noCmdBold> command.

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

  Workaround: Use the **show ip route** command without x.x.x.x.

- CSCtz59615

  Symptom: The IPv6 route does not get installed in the IPv6 VRF routing table.

  Conditions: This symptom is seen in a RADIUS Framed-IPv6-Route.

  Workaround: There is no workaround.

- CSCtz61556

  Symptom: ATM local switching segments do not come up after changing the encapsulation on both interfaces.

  Conditions: This symptom is seen in ATM VC local switching. If the encapsulation on both the ATM VC segments are changed, the segments remain in DOWN state.

  Workaround: There is no workaround.

- CSCtz61599

  Symptom: After adding the performance-monitor policy map under the port channel interface, it continuously displays the information that Port-channel1 has more than one active member link:

```
it-wan-agg5-14(config)#int port-channel 1
it-wan-agg5-14(config-if)#$performance-monitor input PERF-MON-port-channel
it-wan-agg5-14(config-if)#$performance-monitor output PERF-MON-port-channel
it-wan-agg5-14(config-if)# Port-channel1 has more than one active member link
Port-channel1 has more than one active member link
```

  Conditions: This symptom is observed after the performance-monitor policy map is added under the port channel interface.

  Workaround: There is no workaround.

- CSCtz63421

  Symptom: Dynamic update of the encapsulation tag to Single Vlan on Trunk EFP Configured interface must not be allowed.

  Conditions: 1. Configure range of VLANS in Encap tag on trunk efp interface. 2. Change Encapsulation dynamically from range of Vlans to single Vlan encap tag. 3. Check running Configs of Trunk interface.

Workaround: There is no workaround.

- CSCtz63699

  Symptom: In some scenarios, the VRRP "owned" address state is not correctly represented within the "default" VRRS pathway. Additionally, there are various scenarios in which "owned" address conflict checking is not correctly carried out.

  Conditions: These symptoms are only exhibited when a user is using an "owned" address within the VRRP group. An "owned" address is a VRRP virtual address that is equal to one of the addresses configured on the interface.

  Workaround: Use a unique VRRP group address that does not conflict with any of the interface addresses or another address within the same VRF.

- CSCtz63968

  Symptom: The dialer pool is removed from the Ethernet interface.

  Conditions: Crashes occur after the timer expires for PADI. It seems the session was not cleared properly.

  Workaround: There is no workaround.

- CSCtz64836

  Symptom: The **debug redundancy idb-sync-history** command does not work.

  Conditions: The "**debug redundancy idb-sync-history**" command does not work.

  Workaround: There is no workaround.

- CSCtz65370

  Symptom: When performing an RP switchover with a large number of DMVPN sessions (> 3K), ESP40 may reload.

  Conditions: The issue occurs during an RP switchover with many DMVPN sessions.

  Workaround: Clear the IPSec sessions before performing an RP switchover.

- CSCtz67151

  Symptom: The IP SLA responder process causes high CPU utilization.

  Conditions: Configuring a permanent address in the IP SLA responder before enabling the responder can cause High CPU utilisation. To recreate, perform the following configs: i`n responder ip sla responder no ip sla responder ip sla responder udp-echo ipaddress A.B.C.D port XXXX To recover from high cpu, ip sla responder no ip sla responder udp-echo ipaddress A.B.C.D port XXXX`

  Workaround: Ensurethat you enable the responder before programming the permanent addresses, or do not use the permanent addresses.

- CSCtz67726

  Symptom: Single probe ID is not permitted on the **ip sla group schedule** command. Entering the same as probe ID under the **ip sla group schedule** command in the format of the ID is acceptable but this will be displayed as a single probe ID on the running configuration.

  Conditions: This issue is seen while using a single probe ID under the **ip sla group schedule** command.

  Workaround: Use the **ip sla schedule** command for the single probe ID.

- CSCtz67785

  Symptom: The Cisco ASR 1000 Series Aggregation Routers may experience a CPP crash.

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

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

- CSCtz69913

  Symptom: NHRP packets received from a DMVPN tunnel using tunnel protection are dropped on a Cisco ASR 1000 Series Aggregation Routers when the VRF-Aware Service Infrastructure (VASI) interface is configured and the IPSec traffic is traversing the VASI interface. This only happens when using VASI in combination with tunnel protection on the tunnel interface. The NHRP packets are decrypted correctly, but are dropped at the tunnel interface, and the drop counter shows the following drop reason:

```
show platform hardware qfp active statistics drop | e _0_.*_0_
------------------------------------------------------------------------ Global
Drop Stats                          Packets                Octets
------------------------------------------------------------------------
UnconfiguredIpv4Fia 6734
```

  Conditions: The issue occurs when the VASI interface configuration is used for Tunnel protection.

  Workaround: 1) Use a dynamic crypto map on the physical interface. However note that this may cause issues with the spoke behind NAT. 2) Disable VASI, if possible.

- CSCtz69986

  Symptom: The ESP free memory of the ASR 1000 Series Aggregate Services Routers slowly decreases over time (~ 7MB per day).

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

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

- CSCtz70973

  Symptom: The Cisco ASR1002-X Router or ESP100 may reload unexpectedly.

  Conditions: The issue is typically observed when a large number of interfaces are present.

  Workaround: There is no workaround.

- CSCtz71084

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

  Conditions: This symptom is observed in a topology where CE0 and CE1 advertise the same prefixes:

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

  Workaround: Hard clear.

- CSCtz71087

  Symptom: Multiple outside global addresses are assigned the same outside local address.

  Conditions: This issue occurs in a outside dynamic mapping configuration, when running ALG traffic hitting the dynamic mapping, multiple outside global addresses are assigned the same outside local address.

Workaround: Clear the **ip nat translation *** command.

- CSCtz71208

  Symptom: On a Cisco ASR1000 Series Aggregation Services Router, once the error `CPP_FM-3-CPP_FM_TCAM_ERROR` is seen, the only way to recover TCAM is to reload the router. Removing the configuration leading to TCAM exhaustion is not enough.

  Conditions: This is seen after the TCAM is exhausted. This bug pertains only to recovery from exhaustion, not the exhaustion itself. For information about the latter, that, please see CSCtz33305. Deny Statements could exhaust the TCAM entries.

  Workaround: Reload the router.

- CSCtz73450

  Symptom: Multiple <CR> options for the **snmp-server enable traps mac-notification change move threshold**" command results in the following error message:

  ```
  Ambiguous command.
  ```

  Conditions: When trying to configure the **snmp-server enable traps mac-notification change move threshold** command, the parser fails to process the command properly and results in an `Ambiguous command` message.

  Workaround: The user may turn on the **snmp-server enable traps mac-notification change move threshold** command along with other traps by configuring `snmp-server enable traps` and then removing the other unwanted commands. But the user will be unable to remove the commands from the configuration for the same reason that prevents it from being configured.

- CSCtz74060

  Symptom: The **show platform hardware qfp active feature ess state** command does not display output.

  Conditions: The output is displayed in XML format during ISSU sub-package downgrade from XE3.7.0 to lower releases on 4RU. The output is displayed normally after the upgrade. This condition does not have an impact on the functionality.

  Workaround: There is no workaround.

- CSCtz74310

  Symptom: Although there are no visible symptoms, if someone tries to configure Netsync on a Maverick or CEOP_24xT1E1, it will not work. Netsync is not a supported on Maverick and CEOP_24xT1E1.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: There is no workaround.

- CSCtz74315

  Symptom: The Metronome SPA is not supported on Kingpin.

  Conditions: The Metronome SPA fails to come up on Kingpin chassis.

  Workaround: There is no workaround.

  Further Problem Description: The Metronome SPA is not supported on Kingpin. The Netsync feature is supported on hybrid SPA.

- CSCtz74685

  Symptom: A router crash is observed on Y1731 DM.

  Conditions: This symptom is seen when the 1DM session is started.

Workaround: There is no workaround.

- CSCtz75230

  Symptom: When the remote VLAN interface is unshut, with IPv4 data traffic being sent continuously to the remote VLAN interface, the corresponding ARP entry is not created.

  Conditions: When using static FRR configuration and disabling the backup route, shut down the remote vlan interface of the primary path, and then wait for the ARP entry to be removed from ASR1000 Series Aggregation Router after the ARP timeout.

  Workaround:

  Method 1: Configure the static ARP entry.

  Method 2: Provide a valid backup route. Method 3: Do not use static FRR.

- CSCtz75371

  Symptom: When the router is configured with script, the BFD sessions remain inactive. If the same configuration is run manually, the BFD sessions come into the UP state.

  Conditions: This issue occurs only when the bug is reproduced with the script.

  Workaround: There is no workaround.

  Further Problem Descriptions:

  1. The inactive sessions come into the active state when the test client is registered or deregistered with BFD manually.

  2. This issue appears to be a timing-related issue.

  3. Further investigation depends on the availability of the test bed.

- CSCtz75380

  Symptom: A Cisco ASR 1000 Series Aggregation Services Router sends malformed RADIUS packets during retransmission or failover to a secondary RADIUS server, for example, Cisco CAR.

  Conditions: This issue occurs during retransmission of RADIUS access requests or if RADIUS packets are sent to a secondary RADIUS server.

  Workaround: There is no workaround.

- CSCtz75433

  Symptom: When the Open Garden ACL on a Cisco ASR 1000 Series Aggregation Router with ISG functionality is modified, the ACL allows all traffic instead of only Open Garden permit entries.

  Conditions: This issue occurs when at least one unauthorized session is open when the ACL is modified.

  Workaround: Clear all the sessions.

- CSCtz75816

  Symptom: NBAR Field Extraction (AKA collect through IPFIX) does not work for flows over IPv6 tunnels.

  Conditions: This is relevant when configuring NBAR to classify inside the tunneled IPv6 flows. This is anyway not fully supported in the AVC eco-system in XE3.7.

  Workaround: There is no workaround.

- CSCtz77171

  Symptom: Subscriber drops are not reported in Mod4 Accounting.

Conditions: This symptom is seen on the checking policy map interface for account QoS statistics on a port channel subinterface.

Workaround: There is no workaround.

- CSCtz80643

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

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

  Workaround: There is no workaround.

- CSCtz82591

  Symptom: IPv6 multicast internal tunnel numbers conflict with user-configured tunnel numbers.

  Conditions: When user-configured tunnel numbers are in a low range, and the number of internal tunnels being created by IPv6 multicast overlaps with user-configured tunnel numbers on reload, the **nvgen** commands fail.

  Workaround: User-configured tunnel numbers should start at a high value range to avoid conflicting with internal tunnels.

- CSCtz82711

  Symptom: Datapath session crashes.

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

  Workaround: There is no workaround.

- CSCtz83062

  Symptom: Removing and attaching bandwidth percent configurations under a policy-map results in an error message.

  Conditions: This issue occurs when you peform the following procedure:

  1. Create a policy that has bandwidth percent for both user-defined classes and a class default that adds up to 100 percent.

  2. Attach to the interface.

  3. Remove one of the user-defined classes and attempt to reattach the same class with the same bandwidth percent value again.

  Workaround: There is no workaround.

- CSCtz83221

  Symptom: Either the active RP or the standby RP route processor crashes.

  Conditions: This symptom is seen during the configuration or removal of ATM virtual circuits.

  Workaround: There is no workaround.

- CSCtz85102

  Symptom: Packets with the L2 multicast address and L3 unicast address combination cannot be forwarded by the L2TPv3 tunnel on the Cisco ASR 1000 Series Aggregation Router.

  Conditions: This symptom is observed with packets having the L2 multicast address and L3 unicast address combination. This issue is seen in all Cisco ASR 1000 Series Aggregation Services Routers.

Workaround: There is no workaround.

- CSCtz86747

  Symptoms: The xxx router crashes.

  Conditions: This symptom is seen when all the user-defined class maps with live traffic are being removed.

  Workaround: Close the interface first before removing the class map.

- CSCtz87676

  Symptom: The ARP request to the same ip address in different VRFs is incorrectly rate limited. For example: `ping vrf 2001 172.16.0.2 repeat 100 timeout 0 ping vrf 2002 172.16.0.2 repeat 100 timeout 0 ping vrf 2003 172.16.0.2 repeat 100 timeout 0 ping vrf 2004 172.16.0.2 repeat 100 timeout 0`. From the debug arp output, you can see ASR1000 generates only 1 arp request in 2 seconds (0.5 pps) `*Apr 29 03:10:44.932: IP ARP: sent req src 172.16.0.1 *Apr 29 03:10:46.901: IP ARP: sent req src 172.16.0.1 *Apr 29 03:10:48.879: IP ARP: sent req src 172.16.0.1 *Apr 29 03:10:51.004: IP ARP: sent req src 172.16.0.1 *Apr 29 03:10:53.078: IP ARP: sent req src 172.16.0.1 *Apr 29 03:10:55.105: IP ARP: sent req src 172.16.0.1` <snip> Per the design, the arp request to the same ip address in the same VRF is 0.5pps. But when the ip address appears in different VRFs, the ARP request rate should be 0.5 PPS in each VRF.

  Conditions: Day 1 issue.

  Workaround: static arp.

- CSCtz89337

  Symptom: Two paths with the same nexthop are marked and advertised when the all option is set. All paths advertised should have a unique NH.

  Conditions: The issue occurs when there are two paths with the same nexthop.

  Workaround: There is no workaround.

- CSCtz89485

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

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

  Workaround:

  1. Force a HSRP switchover so that the initial standby router takes activity.

  2. Remove and readd HSRP NAT mappings on the newly active router.

  3. Force an HSRP switchover back to the initial active router.

- CSCtz89608

  Symptom: A router that is operating in an ISG environment experiences a crash due to memory corruption.

  Conditions: This symptom occurs within the SSS context.

  Workaround: There is no workaround.

- CSCtz89697

  Symptom: The SIP-400 crashed.

Conditions: This issue occurs because of accessing the NULL pointer in a timer wheel. However, the trigger that contributes to the NULL pointer has not yet been determined. I have added the Eng-notes which has the code analysis for this crash.

Workaround: You can prevent the crash by adding the NULL check condition before calling tw_timer_stop API.

- CSCtz90000

  Symptom: "service-policy type performance-monitor inline input" is applied to a range of interfaces.

  Conditions: Range interface mode may reload a switch if perf-mon inline is applied.

  Workaround: Do not use teh range command option. Apply inline command one at one interface at a time.

- CSCtz90909

  Symptoms: A router crashes when the **no l2 vfi** *vfi-name* **point-to-point** command is run.

  Conditions: This symptom occurs while unconfiguring l2 vfi.

  Workaround: There is no workaround.

- CSCtz92606

  Symptom: The MFR memberlinks-T1 serial interfaces created under a CHOC12 controller do not get decoupled from MFR even after the MFR bundle interface is deleted. After the MFR bundle interface is reconfigured, the memberlinks do not appear under it.

  Conditions: This symptom is seen in MFR with memberlinks as T1 serials from CHOC12 sonet controller.

  Workaround: Unconfigure and reconfigure the encapsulation frame-relay MFRx under each memberlink after reconfiguring the MFR bundle interface.

- CSCtz93922

  Symptom: An XConnect virtual circuit may be down on one peer while it is up on the remote peer. The output of the **show mpls l2 transport vc detailed** command indicates that it is in the LruRrd state and that the last status it received from the remote peer is pw-tx-fault.

  Conditions: This symptom has been observed when both the attachment circuit and core-facing interfaces are on the same module and that module is reset using the **hw-module module** *module* **reset** command, and the remote peer is running Cisco IOS Release 15.2(02)S or later.

  Workaround: Run the **shutdown** command followed bythe **no shutdown** command on the attachment circuit.

- CSCtz94902

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

  Conditions: This symptom occurs on the line card.

  Workaround: Reset the line card.

- CSCtz95698

  Symptom: The standby router by the BGP design remains in the read/write mode after it gets out of the read only mode both in the Active RP and the Standby RP. The read/write mode might, in some timing situation, become the startup state of the new Active RP after SSO. Whereas a fresh reload starts with the read only mode. This read/write startup state is not a desirable state by BGP code design. Hence, this DDTS introduces a new read/scan state for the Standby RP. With this fix the Standby RP stays in the read/scan state and does not change to the read/write state.

Conditions: This is a timing situation when the BGP standby RP after switchover might start best-path or update activity with stale RW mode, then get into RO before finally getting back to the operational RW mode again. This may at times cause unnecessary path updates to go out immediately after switchover (in the stale RW mode, carried forward from its Standby state) only to be replaced with the fully operational best-path updates, once the new Active RP gets to the fully operational RW mode.

Workaround: There is no workaround.

- CSCtz95995

  Symptom: If the router receives the same prefix or masks with the same AD, the code of route origin in the **show ip route** command is overwritten.

  Conditions: This issue occurs at L2TP situation, and can be shown on 12.4(25f) or 15.1(4)M4.

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

- CSCtz96167

  Symptom: The QoS DSCP cases fail.

  Conditions: This symptom is observed in a QoS profile (with 31 as the DSCP value configured under the SBE) but DSCP bit is still sent as 0.

  Workaround: There is no workaround.

- CSCtz96504

  Symptom: Some of the backup VCs go down after SSO.

  Conditions: This symptom occurs only on a scale scenario, for example, by creating 500 primary VCs and 500 backup VCs.

  Workaround: The backup VCs can be brought to the SB state by issuing the **clear xconnect peerid** *peerid of the PW* **vcid** *vcid* command, although it is not usually recommended.

- CSCtz97093

  Symptom: The multilink input counters are not increasing.

  Conditions: The issue occurs when .... it is used as the IPv6 DmVPN tunnel source.

  Workaround: There is no workaround.

- CSCtz97244

  Symptom: IPSLA video operation with VRF support does not receive any packets.

  Conditions: This symptom occurs whenthe **no emulate** command is specified with the input interface.

  Workaround: Use the **emulate** command to specify the input interface that has access to the VRF.

- CSCtz98255

  Symptom: The BGP incorrectly accepts the **route-reflector-client** configuration under neighbor CLI if the neighbor is configured to be eBGP. There is no functionality loss, but the command should not be accepted.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: Remove the incorrect configuration.

- CSCtz98347

Symptom: When ISI-S is configured to run Level 2, the IS-IS LFA does not create repair path if the total metric to a prefix is 1024.

Conditions: This issue was found with 15.2(2)S, and when the ISIS metric is more than 1024 and configured to run Level 2.

Workaround: Ensure that the total metric to a prefix is less than 1024, or use a narrow metric setting.

- CSCtz99914

  Symptom: Traffic drops on MLP interfaces with QoS after a system reload.

  Conditions: Reload.

  Workaround: Use the **Shut** and **no shut** commands in the multilink bundle after reload if the tail drops on the interface are displayed.

- CSCua01375

  Symptom: Certificate validation fails when CRL is not retrieved.

  Conditions: This impacts ASR when configured to use a VRF.

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

- CSCub01576

  Symptom: The ESP reloads on the Cisco ASR 1000 router due to ucode crash.

  Conditions: This symptom is observed on the Cisco ASR 1000 Series Aggregation Routers where the Layer 4 Redirect feature is configured. This problem was firs seen in Cisco Release 15.2(01)S. This issue may not be seen at all in some customer environments, but may be seen about once a week in medium-sized high CPS ISG production networks.

  Workaround: There is no workaround.

- CSCua01641

  Symptom: The NAS-IP address in the RADIUS accounting-on packet is 0.0.0.0:

  ```
  RADIUS:  Acct-Session-Id    [44]  10  00000001 RADIUS:  Acct-Status-Type    [40]  6
  Accounting-On           [7] RADIUS:  NAS-IP-Address     [4]   6   0.0.0.0
  RADIUS:  Acct-Delay-Time     [41]  6   0
  ```

  Conditions: This occurs when you restart the router.

  Workaround: There is no workaround.

- CSCua02783

  Symptom: Get/Walk on PROCESS-MIB fails.

  Conditions: This issue occurs when you upgrade the device from 3.5 to 3.6.

  Workaround: Reload the device.

- CSCua03201

  Symptom: If the VPN ID of an existing Virtual Forwarding Interface (VFI) is changed on a dual RP system, and then a stateful switchover (SSO) is performed, the new standby router may repeatedly reload.

  Conditions: This symptom is observed in Cisco IOS Release 15.2(2)S and Cisco IOS XE Release 3.6.0S and later.

  Workaround: In order to configure a new VPN ID for a VFI, completely remove the existing VFI and reconfigure it.

- CSCua03452

  Symptom: The CLI displays the wrong queue_depth and qlimit values.

  Conditions: The issue occurs when you issue the show platform hardware qfp active interface bqs queue output default interface GigabitEthernet0/1/0 linkdown command.

  Workaround: There is no workaround.

- CSCua03521

  Symptom: Router reloaded.

  Conditions: This issue occurs in some situations where IPV6 address compression fails, and Cisco IOS attempts to restore the previous ACL, but fails.

  Workaround: Rearrange the ACLs.

- CSCua04049

  Symptom: If a capture is stopped because of the limits reached, and the capture is started immediately, the capture fails to stop.

  Conditions: This symptom occurs after the immediate reactivation of a capture.

  Workaround: Clear the buffer before reactivating the capture or wait for a minimum of 5 seconds before reactivating a capture point.

- CSCua04277

  Symptom: IPv6 multicast routes do not get installed correctly.

  Conditions: This issue occurs when you perform the following procedure:
  1. Enable IPv6 multicast.
  2. Configure the IPv6 addresses on the interface.
  3. Configure RIP on these interfaces. Sometimes, the IPv6 route learned from RIP could be missing in the IPv6 multicast routing table.

  Workaround: There is no workaround.

- CSCua04991

  Symptom: The parser chain for the **show application ip route** command is broken for topology.

  Conditions: This issue is visible when topology is enabled in the router.

  Workaround: There is no workaround.

- CSCua06023

  Symptom: Some of WBX image builds are failing.

  Conditions: The issue does not occur in a specific condition.

  Workaround: There is no workaround.

- CSCua06026

  Symptom: The EIGRP routes are not getting redistributed in OSPF.

  Conditions: Stops working intermittently.

  Workaround: Redistribute the connected networks in OSPF.

- CSCua06598

  Symptom: Router may crash with breakpoint exception.

  Conditions: This symptom is observed whenthe SNMP polls the IPv6 MIB inetCidrRouteEntry and a locally sourced BGP route is installed in IPv6 RIB.

Workaround: Disable SNMP IPv6 polling.

- CSCua06804

  Symptom: IPv6 trace route shows incorrect 2nd hop IP address.

  Conditions: Over the interAS network.

  Workaround: There is no workaround.

- CSCua06874

  Symptom: Certain connected routes within a VRF are not installed into the EIGRP topology table (and advertised) although they are in the VRF routing table and are shown as connected.

  Conditions: This issue is seen when you use the **ip vrf receive <***vrf-name***>** command under the connected interface that is to be advertised by the EIGRP.

  Workaround: There is no workaround.

- CSCua07184

  Symptom: On a Cisco ASR1000 Series Aggregation Router with stateful NAT configuration and using inter-chassis redundancy, removing VRF causes the mapping ID to be locked when trying to apply the NAT rules again: %Snat mapping ID 1 in use %Snat mapping ID 2 in use. The NAT rules that were automatically deleted and that customer want to re-apply : ip nat inside source list <ACL name> pool <pool name> redundancy 1 mapping-id 1 vrf <vrf name> overload.

  Conditions: This issue occurs when the following tasks are performed:
  - Remove the VRF using the **no ip vrf** *vrf name* command. All the NAT configurations related to this VRF are deleted.
  - Restore the VRF configuration, and add IP VRF definition.
  - When you try to add the NAT VRF-related configuration, the mapping ID gets locked.

  Workaround: Unconfigure the **ip nat inside source** command before deleting the IP VRF, as described here:
  1. Remove the NAT configurations from the Inside and Outside interfaces.
  2. lear ip nat trans.
  3. Remove NAT rules (no ip nat inside source xxxx xxxx xxx)
  4. Remove and readd the VRF configuration.
  5. Readd the NAT rules and the NAT configurations on the interfaces.

- CSCua07228

  Symptom: Locally generated traffic is not encrypted when a crypto map is applied to the LISP interface.

  Conditions: The issue occurs when GET VPN or the static crypto map is configured on the LISP interface to encrypt traffic between the LISP EIDs.

  Workaround: There is no workaround.

- CSCua07367

  Symptom: When retrieving session information from the VPDN management MIB, some sessions are missing. In addition, the SNMP walk fails to get terminated, instead returning the same sessions repeatedly.

  Conditions: This issue is found in Cisco IOS versions 15.2(01)S01 and later, 15.2(02)T1 and later, 15.1(04)M4 and later, and 15.0(01)M and later.

  Workaround: There is no workaround.

- CSCua07502

  Symptom: The throughput on a multiple member-link MLPPP bundles with links of differing bandwidth may be slightly less than expected due to a complication inthe load balancing algorithm due to mixed bandwidth links. Note that throughput degradation is minimal. The issue was first seen in 15.2(02)S01, but was addressed in Release 15.2(02)S02. Therefore, Release 15.2(02)S01 is the only release with this symptom.

  Conditions: The issue occurs if the MLPPP bundle has multiple member-link MLPPP bundles with links of differing bandwidth.

  Workaround: There is no workaround.

- CSCua08206

  Symptom: VCs (configured with VPLS) on the standby RP in down state.

  Conditions: core link flap.

  Workaround: clear xcon all

- CSCua08027

  Symptom: Tracebacks appear on Cisco ASR 1000 Series Aggregation Services Routers when LI is used with SNMP-based TAP. This occurs from Cisco IOS XE35 Release

  Conditions: This issue occurs when SNMP-based LI is used and the routers are running versions XE35 or later.

  Workaround: There is no workaround.

- CSCua09443

  Symptom: The MLPPPoLNS (L2TP) packet transmit action does not handle the packet transmit operation correctly when the MLPPPoLNS packet is being sent via MPLS VRF (that is, the L2TP tunnel is in a VRF). In the Cisco ASR1000 Series Routers 15.1(3)S and 15.2(1)S release trains, the packet is transmitted as expected, but the MLP Tx ESS Packet Drop statistics may be seen incrementing and the MLP Tx Unfragmented Packet statistics for the bundle indicate that no packets have been transmitted (even though they are likely to have been transmitted). Problem would in most cases be transparent in this release train but MLPPP statistics would be incorrect. In the Cisco ASR 1000 Routers 15.2(2)S release trains, if multilink fragmentation, interleave, or both are DISABLED, the behavior will be the same as in the release trains described earlier. If multilink fragmentation, interleave, or both are ENABLED, the first MLPPP fragment will be sent, but not the remaining fragments. The peer router is also likely to detect lost MLPPP fragments.

  Conditions: This issue occurs when the MLPPPoLNS packet is sent via MPLS VRF (that is, L2TP tunnel is in a VRF).

  Workaround: There is no workaround.

- CSCua09653

  Symptom: Snmp-server host x.x.x.x public bgp.

  Conditions: Functionality is not broken but CLI is not NVGened. However, when router is reloaded functionality would not work.

  Workaround: There is no workaround.

- CSCua10815

  Symptom: A leak is seen in CPP memory, and the FP crashes.

  Conditions: This symptom is observed when the IPSec WCCP is configured. Due to a large number of debug log messages in the cpp_cp_F0-0.log file, there is a memory leak in the CPP, and the FP crashes.

Workaround: There is no workaround.

- CSCua11924

  Symptom: Under certain conditions, a Cisco ASR1000 Series Aggregation Router may send ICMP type 3 code 4 (unreachable, fragmentation needed, but with the DF bit set) packets with a wrong source IP address, that is, the IP address configured on the ingress interface of the original packet (which is too big and cannot be fragmented) instead of an IP address belonging to an interface in the VRF the packet is destined for.

  Conditions: This issue occurs when MPLS VPN is used and the big packet enters the router through an MPLS interface, and when the egress interface has a lower MTU and belongs to a (nonglobal) VRF.

  Workaround: If possible, do not filter ICMP unreachables based on the source IP address in the network between the Cisco ASR1000 Series Agregation Router and the sender. Apply a route map to ignore the DF bit, allowing the big packets to be fragmented, or in the contect of TCP traffic, apply the **ip tcp adjust-mss <***value***>** command to lower the TCP MSS of the sending host.

- CSCua12396

  Symptom: IPV6 multicast routing is broken in master switchover scenarios with a large number of members in the stack. The issue is seen on platforms such as Cisco ® Catalyst ® 3750-E Series Switches and the Cisco Catalyst 3750-X Series Switches that support IPV6 multicast routing.

  Conditions: The issue occurs when IPV6 multicast routing is configured, multicast routes are populated, and traffic is being forwarded. In master switchover, synchronization between the master and members is disrupted. This is seen only in IPv6 multicast routing; it is seen in a 9-member stack and either during the first or the second master switchover. No issues are seen in IPv4 multicast routing.

  Workaround: Enable IPv6 multicast routing when you have a deployment with less members in the stack.

- CSCua12467

  Symptom: Multicast operation and sub-opers return OK even though errors occurred.

  Conditions: OK return code even though stats are not populated (for various error conditions)

  Workaround: Display problem only. Fix underlying error and results will be OK.

- CSCua13082

  Symptom: A PPPoE client's host address is installed in the LNS' VRF routing table with the **ip vrf receive** *VRF NAME* command supplied either via RADIUS or in a virtual template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.

  Conditions: This issue does not occur under a specific condition. The only condition that exists is the virtual access interface with **ip vrf receive** *VRF NAME* configured via the virtual template or the RADIUS profile.

  Workaround: There is no workaround.

- CSCua13273

  Symptoms: The Cisco ASR 1000 Series Aggregation Services Routers may experience an RP crash when the **show crypto ipsec security** command is used.

  Conditions: This issue occurs when the Cisco ASR 1000 Series Aggregation Routers run an affected version of Cisco IOS-XE, and an administrator issues the **show crypto ipsec security** command.

  Workaround: There is no workaround. This issue requires that an authenticated Level 15 administrator or a configured AAA user with access to the **show crypto ipsec security** command to issue the command. This is being treated as a functional issue by PSIRT and the BU, and will be

resolved in a future version of Cisco IOS-XE. PSIRT Evaluation. Cisco PSIRT has evaluated this issue. This issue does not meet the criteria for PSIRT ownership or involvement, and will be addressed via normal resolution channels. If you believe that there is new information that will cause a change in the severity of this issue, 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

- CSCua13322

  Symptom: Routes for the converted dedicated P sessions are missing after an RP switchover.

  Conditions: Converted dedicated IP sessions are not HA awared. Therefore, after an RP switchover, these sessions will be re-established at the new active RP. Routes are not installed for some of these sessions. As a result, downstream traffic is dropped.

  Workaround: There is no workaround.

- CSCua13418

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

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

  Workaround: Removing filter-autorp resolves the issue. However, you should remove the **pim** and **boundary** commands first and then reapply the PIM and boundary list without the **filter-autorp** keyword. Also, doing this might lead to the redesigning of the topology to meet specific requirements. For example, execute **int Tun X no ip pim sparse-dense mode no ip multicast boundary** *XXXXXX* **filter-autorp** and then **int TuX ip pim sparse-dense mode ip multicast boundary** *XXXXXX*.

- CSCua13551

  Symptom: CAT 6K and ASR 1000 learning candidate default routes from nexus due to which the default route is not being learnt properly and caused an outage.

  Conditions: Nexus is running into a bug CSCtz79151 because of which it is advertising the candidate defaults to its downstream neighbors.

  Workaround: workaround is to configure ?default-information in xxxx? on the 6500's, where xxx is an acl denying all default candidates from being learned except 0.0.0.0/0. On 6500 access-list 30 remark Workaround for Nexus_Bug access-list 30 remark Deny all default candidates except DR access-list 30 permit 0.0.0.0 access-list 30 remark Deny all other routes access-list 30 deny any router eigrp 109 default-information in 30.

- CSCua13561

  Symptom: After upgrading to Cisco IOS XE 15.2(2)S, users cannot get the IP address via PPP IPCP from the DHCP pool on the Cisco ASR 1000 Series Aggregation Routers. There is no configuration change.

  Conditions: This issue occurs when you upgrade to Cisco IOS XE 15.2(2)S.

  Workaround: Remove the **vpdn authen-before-forward** command.

- CSCua14569

Symptom: The **ip vrf receive** command is not cloned to VAI from VT.

Conditions: This issue occurs when the **ip vrf receive** command is configured before PPPoE session.

Workaround: Configure once after the session is up.

- CSCua14594

  Symptom: A memory leak is seen when polling for the following PW MIBs:
  `1.3.6.1.4.1.9.10.106.1.5.1.1 (cpwVcPerfTotalInHCPackets) 1.3.6.1.4.1.9.10.106.1.5.1.2 (cpwVcPerfTotalInHCBytes) 1.3.6.1.4.1.9.10.106.1.5.1.3 (cpwVcPerfTotalOutHCPackets) 1.3.6.1.4.1.9.10.106.1.5.1.4 (cpwVcPerfTotalOutHCBytes)`
  `Address Size Alloc_pc PID Alloc-Proc Name 34417B84 308 13774B30 473 SNMP ENGINE AToM VC event trace`

  Conditions: This symptom is observed with Cisco IOS Release 3.6S when the SNMP VC statistics query is polled.

  Workaround: There is no workaround.

- CSCua14640

  Symptom: The configuration order changes after router reload.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: There is no workaround.

- CSCua14821

  Symptom: Traffic loss and see ack-pend when the **show platform software object-manager fp active statistics command** is executed. For example:

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

  Object update: Pending-issue: 0, Pending-acknowledgement: 8
  Batch begin:   Pending-issue: 0, Pending-acknowledgement: 0
  Batch end:     Pending-issue: 0, Pending-acknowledgement: 0
  Command:       Pending-acknowledgement: 0
  Command:       Stale-objects: 0
  ```

  Conditions: UUT is using FP80 and also traffic is Jumbo frame pkt

  Workaround: There is no workaround.

- CSCua14919

  Symptom: IPv6 ISG session in attempting state on STANDBY-rp

  Conditions: Just create one IPv6 ISG session.

  Workaround: There is no workaround.

- CSCua16899

  Symptom: The SFP and SPA modules only may appear to be missing from **show inventory**.

  Conditions: This issue is observed after system bootup.

  Workaround: Reload the SIP. This should reinitialize the SPA and SFP modules.

- CSCua16958

  Symptom: The ha_mgr does not recognize the PEER_PRESENCE/PEER_COMM events between the active and standby servers, leading to the standby server crashing.

  Conditions: Standby router crashes.

  Workaround: There is no workaround.

- CSCua18542

  Symptom: When a service change occurs as ISG, SCE is not ready to accept the CoA. In such a scenario, the ISG resends an update session on the ISG-SCE Bus. The update session is sent, but it does not have the attributes for SCE.

  Conditions: This issue does not occur under a specific condition,

  Workaround: There is no workaround.

- CSCua18679

  Symptom: The Framed IP Address is not included in the accounting start requests for dual stack (IPv4 and IPv6) users and when the IPv4 is coming from a local IP pool. Accounting interims and accounting stop messages always include the Framed-IP-Address attribute (attr(8)). Following commands were configured and were of no help in: **aaa accounting delay-start [all] aaa accounting include auth-profile framed-ip-address**

  Conditions: Dual Stack users and IP address is given from a Local IP pool.

  Workaround: Break any of the condition above: IPv4 users are not affected, even if the IP is coming from a local pool. If the IP address is coming from the radius, with the Framed-IP-Address attribute, it is OK.

- CSCua19207

  Symptom: From Cisco IOS XE Release 3.1, a Cisco ASR 1000 Series Aggregation Router is unable to support class-default shaping on a subinterface used with tunnel QoS.

  Conditions: This issue occurs on a Cisco ASR 1000 Series Aggregation Router when you try to configure class-default shaping on a subinterface used with tunnel QoS.

  Workaround: There is no workaround.

- CSCua19016

  Symptoms: A duplicate XConnect instance (VCID, Peer ID) is accepted when configured on a different interface.

  Conditions: This issue occurs when you use the basic **xconnect config** command.

  Workaround: Do not use the same VCID and Peer ID on two distinct interfaces.

- CSCua19425

  Symptom: The RP crashes at the far end of xx, pointing to a Watchdog Process BGP.

  Conditions: This issue occurs when you perform an FP reload at the near end. EBGP sessions with BFD configured between near end and far end routers.

  Workaround: There is no workaround.

- CSCua20021

  Symptom: The **clear ethernet cfm ais** command with the EVC option does not work.

  Conditions: This issue occurs when you specify the EVC name with the **clear ethernet cfm ais** command.

  Workaround: Use **service** option instead.

- CSCua21049

  Symptom: The recursive IPv6 route is not installed in the multicast RPF table.

  Conditions: This issue occurs in a multicast RPF table.

  Workaround: There is no workaround.

- CSCua21171

  Symptoms: The ping does not pass between a few Distributed LFI over ATM (dLFIoATM) bundles.

  Conditions: This symptom is observed after a few dLFIoATM bundles are configured. Check the ping between bundles and perform a **shut/no shut** of the interface.

  Workaround: There is no workaround.

- CSCua21238

  Symptoms: Cisco IOS crashes @_ipv6_address_set_tentative.

  Conditions: This symptom occurs while unconfiguring the IPv6 subinterfaces during the loading phase of a box with NetFlow configuration.

  Workaround: There is no workaround.

- CSCua22166

  Symptom: The IPv6 reassembly percentage functionality does not work, for example, percentage 100% for EF, EF IPv6 traffic should not be dropped, however it is drops some percentage.

  Conditions: IPv6 neighbor adjacency works abnormal.

  Workaround: Add the **ipv6 neighbor ipv6_address GigabitEthernetx/x/x.vlan_id ipv6_peer_mac** command to the subinterface. The issue does not occur in the latest MCP_DEV release.

- CSCua22825

  Symptom: Routes with interface gateway are not deleted.

  Conditions: Gateway should not fall in the subnet configured on the interface.

  Workaround: Run the **clear ip route** command to delete the routes after the application is deregistered.

- CSCua23262

  Symptom: A BFD crash and major network outage is seen.

  Conditions: Configuring the **no ip route-cache** command on the main interface or subinterface configures the same on all the subinterfaces of that interface, causing the BFD to go down and a major network outage to occur due to slow convergence.

  Workaround: There is no workaround.

- CSCua23997

  Symptom: Continuous ESP crash is seen after packets are dropped because of unsupported OCE.

  Conditions: This issue is observed when the OCE is unsupported.

  Workaround: There is no workaround.

- CSCua24689

  Symptom: Fragments are sent without labels resulting in packet drops on the other side.

  Conditions: This symptom is observed under the following conditions:

  - MPLS-enabled DMVPN tunnel on egress
  - VFR on ingress

  Workaround: Disable VFR, if possible.

- CSCua25041

Symptom: The entPhysicalIsFRU of the 6-port built-in GE SPA in the Cisco ASR1002-X Router is false. As a result, the built-in SPA is shown in the cefcModuleTable.

Conditions: This issue occurs when the SNMP is queried on entPhysicalIsFRU or cefcModuleTable on the ASR1002-X chassis.

Workaround: There is no workaround.

- CSCua26487

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

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

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

  See the below configurations.

```
snmp-server view iso included
snmp-server view ceeSubInterfaceTable excluded
snmp-server community view nterfaceTable excluded
snmp-server community view Symptom.
```

- CSCua27842

  Symptom: A Cisco ASR 1000 Series Aggregation Service Router crashes in firewall code due to NULL l4_info pointer.

  Conditions: This symptom occurs when a Cisco ASR 1000 Series Aggregation Router acts as the MPLS L3VPN UHP. It crashes because FW/NAT requires l4_info to be set. This issue is triggered when the following features are configured:

  - MPLS L3VPN (PE)
  - Zone-based FW/NAT
  - MPLS and MP-BGP load balance configured towards the upstream router.

  Workaround: There is no workaround.

- CSCua27852

  Symptom: Traffic loss is seen in the pure BGP NSR peering environment.

  Conditions: This symptom is seen on a Cisco router that is running Cisco IOS Release 15.2(2)S, and the BGP peerings to CEs and RR are all NSR enabled.

  Workaround: Enable the **bgp graceful-restart** command for RR peering.

- CSCua28910

  Symptom: A VRF flap with IPv6 MTU configuration causes IPv6 table ID to be disabled and packets to be dropped.

  Conditions: This issue occurs when you configure IPv6 MTU 1280 under interface change interface vrf.

  Workaround: Remove IPv6 MTU 1280 or change MTU to another value.

- CSCua29001

  Symptoms: The ANCP truncated line rate is not seen on the standby router. Also, the policy application differs from that of the active router.

  Conditions: This symptom occurs whenthe **ancp truncate value** CLI is enabled, and port ups are received on BRAS.

  Workaround: There is no workaround.

- CSCua29095

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

  Conditions: This symptom occurs while booting the image.

  Workaround: There is no workaround.

- CSCua30053

  Symptom: Authentication fails for clients due to radius_send_pkt fails, because of low IOMEM condition.

  Conditions: In AAA, minimum IO memory must be 512KB to process a new request. If the memory is less than this, AAA does not process the new Authentication request. This is AAA application threshold. The application barriers are not valid in case of dynamic memory. As such conditions are removed for NG3K platform.

  Workaround: There is no workaround.

- CSCua32893

  Symptom: Ucode and cpp_cp_svr crash is seen on the Cisco ASR 1002 Routers (standby) while scaling to 0.5 million NAT64 translation.

  Conditions: This symptom is observed with high scaling.

  Workaround: There is no workaround.

- CSCua33788

  Symptom: The router does not pass multicast traffic consistently; only some traffic is passed.

  Conditions: This symptom occurs when you configure 255 EVCs spanning across different slots on the router.

  Workaround: There is no workaround.

- CSCua34428

  Symptom: When a routed port is configured, the CC messages are not generated because the local MEP is in I state instead of Y state for these messages. Hence RMEP is not learnt.

  Conditions: Apply routed port and you will hit the issue.

  Workaround: Perform a **shut/no shut** operation.

- CSCua34638

  Symptom: A crash is seen on RP2.

  Conditions: This symptom is observed when the **show platform software shell command package** command is executed. It impacts only the RP2 (x86_64_*) image.

  Workaround: There is no workaround.

- CSCua35446

  Symptom: Gigabit 0/5/0 interface is displayed in PRIME software.

  Conditions: System being up.

  Workaround: There is no workaround.

- CSCua36463

  Symptom: IPv6 ACL Extensions for dest-option filtered IPv6 traffic that contain hop-by-hop extension.

  Conditions:

Tester---ASR1001---Tester

Platform: ASR1001

Software: IOS-XE3.4.3S.

Workaround: There is no workaround.

- CSCua36540

  Symptom: It is possible for two or more FHRPs (HSRP, VRRP, or GLBP) to use the same IP address as the virtual address for their group.

  Conditions: This issue occurs when two or more FHRPs are configured on an interface and uses the same IP address.

  Workaround: Do not configure different FHRPs on the same interface.

- CSCua37614

  Symptom: The tunnel client endpoint and tunnel server endpoint (66/67) are missing from the RADIUS Access-Accept messages.

  Conditions: This issue is specific to LNS.

  Workaround: There is no workaround other than changing the solution, which is not easy for customer migrations.

- CSCua38237

  Symptom: Router generates PSNP packets with MD5 hash 0x0.

  Conditions: This does not affect less than full size SNPs.

  Workaround: There is no workaround.

- CSCua38597

  Symptom: Private ASN is not removed from AS-PATH.

  Conditions: BGP neighbor must be configured with remove-private-as. The outbound route map must have the continue clause.

  Workaround: Configure the route map without the continue clause.

- CSCua38820

  Symptom: Adding the match protocol attribute p2p-technology p2p-tech-no to a class map causes the service policy to not work:

  ```
  ASR1004(config)#class-map match-all http_attributes_class
  ASR1004(config-cmap)#match protocol attribute p2p-technology p2p-tech-no.
  ```

  Conditions: Do not use the p2p-tech attribute in class map.

  Workaround: There is no workaround.

- CSCua40273

  Symptom: A Cisco ASR 1000 Series Aggregation Services Router crashes when displaying MPLS VPN MIB information.

  Conditions: This issue occurs on the routers running software release 15.1(02)S software.

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

- CSCua40790

  Symptom: Memory leaks are observed when SNMP polls the cbgpPeer2Entry MIB.

  Conditions: This issue occurs when the BGP v4 neighbors are configured.

Workaround: There is no workaround.

- CSCua41398

  Symptom: The SUP720 crashes.

  Conditions: Occurs while issuing the **sh clns** interface.

  Workaround: There is no workaround.

- CSCua41519

  Symptom: The following error message is displayed after the **write mem** command is applied on the active supervisor:

  ```
  HA_CONFIG_SYNC-3-GENERAL
  PFREDUN-3-STANDBY_OUT_OF_SYNC
  Active and Standby are out of sync.
  -Traceback= 42AE1044z 42F05BE0z 4083C860z 40842DA0z 42F11CA4z 40853BD0z 420DAFD4z
  41C080C0z 41C080A4z.
  ```

  After this the standby xx reloads.

  Conditions: This occurs in a Cisco 7609 Router running Release 15.2(1)S of

  Workaround: There is no workaround.

- CSCua41828

  Symptom: The **show ipv6 traffic counter** command displays a larger number of sent neighbor unreachables than those actually sent.

  Conditions: This issue occurs when a packet has a link-local source address and whose destination address is in a remote network is received by a Cisco ASR 1000 Series Aggregation Services Router.

  Workaround: There is no workaround.

- CSCua43930

  Symptom: The checksum value parsed from the GRE header is not getting populated causing the GRE tunnel checksum test case to fail.

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

  Workaround: There is no workaround.

- CSCua44188

  Symptom: The wildcard source IP address within the ISG control class map is not shown in the running configuration although the actual class map works correctly in the configuration. If the router is reloaded, the source address is not parsed from the startup configuration into the running configuration.

  Conditions: This issue occurs when the wildcard address "0.0.0.0 0.0.0.0" is used in configuration as shown in the following configuration sample:

  ```
  class-map type control match-any IP-Address-Ranges
  match source-ip-address 0.0.0.0 0.0.0.0
  ```

  This is parsed correctly but shows up in the running configuration as:

  ```
  class-map type control match-any IP-Address-Ranges
  match source-ip-address.
  ```

  Workaround: There is no workaround.

- CSCua44483

  Symptom: Mcast stops sending for all groups after all the flows have ceased due to timeout.

Conditions: This issue occurs during a normal operation, after the senders have stopped sending and/or flows have timed out as normal.

Workaround: Disable and re-enable MCAST routing.

- CSCua45114

  Symptom: Default sessions will not get established when you apply VRF as a service to the default policy. VRF can be applied to a default session only by assigning a VRF on the access interface. However, in dedicated sessions, one cannot apply a VRF on the access interface and perform a VRF transfer at the same time.

  Conditions: This symptom is seen when the access side interface is in the default VRF. The VRF is applied as a service to the default policy.

  Workaround: There is no workaround.

- CSCua45278

  Symptom: Routing table entries are displayed as static instead of connected on a Cisco 7600 Router acting as a DHCP relay agent when **ip dhcp route connected** is configured.

  Conditions: This is observed after a Supervisor failover occurs with DHCP clients.

  Workaround: There is no workaround.

- CSCua45303

  Symptom: Bogus cloned sessions after QFP memory is exhausted.

  Conditions: In 128K lite sessions, clearing the default session may lead to QFP memory exhaustion. When this happens, bogus cloned sessions are seen.

  Workaround: There is no workaround.

- CSCua45690

  Symptom: When OSPF NSR is configured, bulk synchronization fails with the following error message:

  ```
  %OSPFv3-STDBY-3-CHKPT_STBY_LSDB_INVALID CONDITION OSPF.
  ```

  Workaround: Perform the following procedure:

  a. Copy the <CmdBold>nsr<NoCmdBold> command into the original configuration
  b. wait to configure <CmdBold>nsr<NoCmdBold> until the adjacencies have reached FULL state.

- CSCua45122

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

  Conditions: This symptom is observed in the multicast even log.

  Workaround: There is no workaround.

- CSCua45548

  Symptoms: The Cisco 2900 Series Integrated Services Routers, Cisco 1900 Series Integrated Services Routers, and the Cisco 3945 Integrated Services Routers crash with s**how ip sla summary** on longevity testing.

  Conditions: This symptom is observed in the Cisco 2900 Series Integrated Services Routers, Cisco 1900 Series Integrated Services Routers, and the Cisco 3945 Integrated Services Routers configured with IPSLA operations. Routers that are idle for a day crash when the **show ip sla summary** commandis issued.

  Workaround: There is no workaround.

- CSCua47980

  Symptom: The **show run vrf** command does not display any OSPFv3 configuration associated with the specified VRF.

  Conditions: This issue occurs when VRF and the OSPFv3 configuration are present in the running configuration.

  Workaround: Use the **show run** command to view the full configuration.

- CSCua48243

  Symptom: The Cisco ASR 1000 Series Aggregation Services Routers logs truncate the IPv6 addresses if the **log** keyword is used in a security ACL.

  Conditions: This issue occurs when a security ACL having the **log** keyword is applied on an interface.

  Workaround: There is no workaround. ACL's functionality is not affected.

- CSCua49389

  Symptom: The IP SLA fails and the log displays the following message:

  ```
  "IPSLA-OPER_TRACE:OPER:10 slaSize less, slaSize = 64, sizeof(slaJitterProbePakV3) =
  92" .
  ```

  Conditions: This issue occurs when the timestamp is enabled and the configured request size is small.

  Workaround: Configure the request data size to a large number and ensure that the minimum request data size is 96.

- CSCua49474

  Symptom: Some TCP segments of a particular length may be forwarded with the wrong packet payload if NAT configured.

  Conditions: NAT configured packets are TCP segments of particular length.

  Workaround: Configure the **ip tcp adjust-mss** to a value that is smaller than the current TCP flow.

- CSCua50961

  Symptom: Pseudowire redundancy cannot bring up the secondary pseudowire that is also configured as the backup on the other side.

  Conditions: No issues in activating pseudowires that are primary on the other side.

  Workaround: Terminate the pseudowires on a different AC and make them as primary. There is no workaround if you want to terminate the pseudowires on the same AC.

- CSCua51775

  Symptom: Adding the **flow-based fair-queue** command to the QoS policy map might cause conditional priority fail to police the traffic when congestion condition happens.

  Conditions: If the service policy has already been attached to the interface, adding the **fair-queue** command to the policy map disables the congestion detection flag setting that is used by the conditional priority traffic class, causing the traffic class to behave like a strict priority traffic class.

  Workaround: Detach and reattach the same service policy to the interface when you add the **fair-queue** command to the policy map attached to the interface.

- CSCua52064

  Symptom: LSMPI-4-INJECT_FEATURE_ESCAPE: Egress IPV6 packet delivered inject path.

Conditions: Traceback is seen when you disable **ipv6 unicast-routing** from the device that is forwarding IPv6 unicast packets.

Workaround: There is no workaround.

- CSCua53381

  Symptom: %CPPOSLIB-3-ERROR_NOTIFY: F1: cpp_cp and %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image: ess-lite-session TBs are intermittently seen when the **clear subscriber session all** command is issued.

  Conditions: The issue occurs when the EAPSIM, L3 Web Authentication, and Walkby sessions are being established concurrently. The issue is reproducible in only one in a thousand sessions.

  Workaround: There is no workaround.

- CSCua53742

  Symptom: LCP echo requests are dropped during severe and constant congestion of an ATM PVC configured as a PPPoE client.

  Conditions: This has been observed on an 887 series router with the ATM interface configured as a PPPoE client when causing constant, severe congestion with a traffic generator.

  Workaround: There is no workaround.

- CSCua53917

  Symptom: On a DualSup Cat4k system, the **show redundancy config-sync failures prc** command consistently reports the following errors:

```
Router#show redundancy config-sync failures prc
PRC Failed Command List
-----------------------
-ip vrf Liin-vrf
! <submode> "vrf"
ip vrf mgmtVrf
! </submode> "vrf"
```

  Conditions: This issue occurs when Cat4k is running Cisco IOS XE with dual supervisors.

  Workaround: There is no workaround.

- CSCua54407

  Symptom: ANCP line rate to some value 'X' for that PPP sub-interface. Then change it to 'Y'. 'X' is not released.

  Conditions: This issue occurs whenever ACNP rate changes.

  Workaround: There is no workaround.

- CSCua54514

  Symptom: Bqs queue output is different for FP10 and FP80.

  Conditions: Output difference is seen while checking the **show platform hard qfp ac fe qos queue out all** command output.

  Workaround: There is no workaround.

- CSCua54689

  Symptom: Router sends IP SLA path-jitter packets with a different source IP that is different from the configured one.

  Workaround: There is no workaround.

- CSCua55691

  Symptom: A Cisco IOS memory leak is observed.

  Conditions: This issue is observed when unconfiguring or reconfiguring BGP AD VFIs.

  Workaround: There is no workaround.

- CSCua55752

  Symptom: Unexpected set ip next-hop is applied on packets subjected to PBR. This happens only if a similar next hop is tracked with multiple tracking objects.

  Conditions: This issue occurs when PBR is applied on the incoming interface and verify-availability is configured.

  Workaround: Avoid configuring same next hop with multiple tracking objects.

- CSCua55797

  Symptom: When the **show running** or **copy running-config startup-config** commands are executed, the **privilege exec level 0 show glbp brief** command causes the memory of ... to be depleted. The configurations display the following message:

  ```
  privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief brief
  brief brief     privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief
  brief brief brief    privilege exec level 0 show glbp GigabitEthernet0/0 brief brief
  brief brief brief    privilege exec level 0 show glbp GigabitEthernet0/0 brief brief
  brief brief   privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief
  privilege exec level 0 show glbp GigabitEthernet0/0 brief brief     privilege exec
  level 0 show glbp GigabitEthernet0/0 brief     privilege exec level 0 show glbp
  privilege exec level 0 show.
  ```

  Removing the configurations display the following message over and over until the Telnet session is terminated:

  ```
  priv_push : no memory available
  ```

  If the configurations are saved and the device is reloaded, the device will not fully boot until the configurations are bypassed.

  Conditions: This issue occurs when you execute the **privilege exec level 0 show glbp brief** command and saving the command.

  Workaround: Reload the router before saving the configurations.

- CSCua56209

  Symptom: Pseudowires (PWs) are not enabled after an SSO.

  Conditions: This is only a specific case where the primary pseudowire path is DN when the active RP coming up, so the backup PW comes to UP state. Later when the primary path is available pseudowire redundancy switchover happens the primary PW becomes UP. At this stage if the Software Switchover happens the PWs on the newly active RP is DN.

  Workaround: Run the **clear xconnect all** command to enable the PWs.

- CSCua56802

  Symptom: QoS does not work on one of the subinterfaces or EVC.

  Conditions: This issue occurs when you configure the HQoS policy on more than one sub-interface or EVC on ES.

  Workaround: Remove and reapply SG.

- CSCua58100

Symptom: The syslog displays the following traceback message:

```
Jun 20 10:05:23.961 edt: %SYS-2-NOTQ: unqueue didn't find 7F3D26BDCCD8 in queue
7F3CA5E4A240 -Process= RADIUS Proxy, ipl= 0, pid= 223 -Traceback=
1#e0ee0ce60492fdd11f0b03e0f09dc812 :400000 873623 :400000 2547652 :400000 20F9217
:400000 6C70C9C :400000 6C69C71 :400000 6C682BC :400000 6C68183  Conditions: Occurs
under the following
```

Conditions: Establish 36k EAPSIM sessions using a RADIUS client on server A, and then establish 36 k roaming sessions using a RADIUS client on server B. The roaming sessions have the same caller station ID, but use a different IP address from that of the EAPSIM sessions.

Workaround: There is no workaround.

- CSCua58072

  Symptom: On some Cisco ASR 1000 Series Aggregation Services Routers, IPv6 BGP next hop is collected with misordered bytes, for example, a nonexisting IPv6 address is displayed for it.

  Workaround: There is no workaround.

- CSCua58324

  Symptom: Pending objects are generated after copying a PWLAN configuration with default sessions to the running configuration.

  Conditions: This issue occurs when a Cisco ASR 1000 Series Aggregation Services Router is initiated with basic startup configuration. Copy the PWLAN configurations to the running configurations.

  Workaround: There is no workaround.

- CSCua58386

  Symptom: The dispersion and delay values are printed wrongly.

  Workaround: The dispersion and delay values are 64-bits values. Configure the **ntp** commands and compare sh ntp association values with SNMP-GETBULK values.

- CSCua59268

  Symptom: When an ESP switchover occurs in an intrabox or interbox setup, the standby ESP gets stuck and does not come up properly.

  Conditions: The **show redundancy application group** <*grp-number*> command on the new standby (previously active) shows the RF state as STANDBY COLD-BULK.

  Workaround: Reload the standby.

- CSCua60078

  Symptom: Issue seen while unconfiguring virtual-template configurations.

  Conditions: This symptom occurs when virtual-template configurations are removed.

  Workaround: There is no workaround.

- CSCua61330

  Symptom: Traffic loss is observed during switchover under the following scenarios:

  - BGP graceful restart is enabled
  - Next hop is learned by BGP

  Conditions: It happens with cisco router loading with XE35 image

  Workaround: There is no workaround.

- CSCua61394

Symptom: The addition and deletion of application route entry fails.

Conditions: This issue occurs when there is an addition and deletion of the same IP address and gateway, but with a failure of different gateway topoids.

Workaround: There is no workaround.

- CSCua61760

  Symptom: When fast reroute is configured, IS-IS inter-area prefixes do not have a repair path.

  Conditions: This symptom does not occur under a specific condition.

  Workaround: There is no workaround.

- CSCua61814

  Symptoms: Overhead accounting configuration needs to be configured on both the parent and child policies, rather than just the parent policy.

  Conditions: This symptom is observed with overhead accounting.

  Workaround: There is no workaround.

- CSCua62545

  Symptom: After attaching an attribute map to a protocol, the same is not reflected at the Collector when the FNF export of the options attribute is enabled.

  Conditions: When the attribute map is configured and an attribute set is done to one or more protocols.

  Workaround: Force an NBAR restart with a reload, protocol pack load, and so on.

- CSCua62550

  Symptom: When the volume and/or time prepaid is applied on PPPoE PTA sessions through auto service, the volume and/or time monitor is not applied on the session.

  Conditions: This issue occurs when the prepaid auto service on the PPPoE PTA session is exhausted.

  Workaround: There is no workaround.

- CSCua63182

  Symptom: Incorrect minimum bandwidth is displayed when 0 kb bandwidth is received from a peer of a different version of xx.

  Conditions: Different behavior in ASR when minimum bandwidth of 0 kb is received from xx.

  Workaround: There is no workaround.

- CSCua64358

  Symptom: When an SVTI uses a loopback interface as tunnel source, the ping fails.

  Conditions: When the tunnel source is the loopback interface, the default MTU setting is 1514, and the ping through this SVTI tunnel is dropped at the corresponding peer box with an error message report.

  Workaround: Change the MTU setting to the physical interface such that the former is the same as that on the loopback interface.

- CSCua64676

  Symptoms: MVPNv4 traffic does not flow properly from the remote PE to the UUT.

  Conditions: This symptom is seen in Agilent traffic on and after the removal/addition of MDT configurations for the MVRFs configured on the UUT.

Workaround: There is no workaround.

- CSCua65067

  Symptom: Apply control policy to identify RP session using unauthorized user name. The policy is applied to both the DHCP and RP sessions.

  Conditions: This issue occurs when the same control policy is used for DHCP sessions.

  Workaround: Create a separate policy for the DHCP sessios and the RP sessions.

- CSCua66308

  Symptom: Classification- related error messages and tracebacks are seen on the CLI console, and the configuration is not downloaded to the data path.

  Conditions: This symptom is observed in large configurations with multiple deny statements.

  Workaround: Observe caution when using deny statements in a configuration.

- CSCua66386

  Symptom: The Cisco ASR 1000 Series Aggregation Services Router do not send an ICMPv6 Unreachable Code One message to a sender when the packets are discarded by an ACL.

  Condition: This issue occurs when you use a Cisco ASR 1000 Series Aggregation Services Router as LNS and deny the packets by an ACL in the virtual template interface.

  Workaround: There is no workaround.

- CSCua66795

  Symptom: A neighbor may not inherit the configuration of a peer group.

  Conditions: When a neighbor has the same configuration before it joins a peer group that is not configured, then it applies only to the session configuration, for example, the configuration does not apply to AF configuration.

  Workaround: Reapply the configuration to the peer group. If it does not work, configure the peer group to a different value, and then configure the peer group to its original value. After this, unconfigure the neighbor, and then reconfigure the neighbor.

- CSCua66870

  Symptom: When changing the RPF neighbor (S,G) in the PIM-dense mode, OIF on (*,G) is pruned unexpectedly.

  Condition: This issue occurs when you use PIM-dense mode.

  Workaround: There is no workaround.

- CSCua67998

  Symptoms: The system crashes.

  Conditions: This symptom occurs after you add or remove a policy map to a scaled GRE tunnel configuration.

  Workaround: There is no workaround.

- CSCua68211

  Symptom: Subclassification of the HTTP traffic (for example, by host, URL, and so on) will sometimes not work on the first transaction of the HTTP flow and will only match in the second request.

  Conditions: This symptom is observed when all the protocols or specific protocols on top of HTTP are enabled, for example, sharepoint, audio-over-HTTP, video-over-HTTP, Windows Azure, Oracle EB-Suite Unsecured, BitTorrent and so on.

Workaround: If you are using subclassification on HTTP, avoid using protocol discovery, FNF, or specifically enabling other protocols that run over HTTP.

- CSCua68825

  Symptom: A Cisco ASR 1000 Series Aggregation Services Router that is configured as LISP xTR might generate large ICMP messages with wrong source address.

  Conditions: When the data packets are encapsulated by LISP xTR, and the encapsulated packet is greater than the egress MTU, a Cisco ASR 1000 Series Aggregation Services Router generate an ICMP reply with the wrong source address.

  Workaround: There is no workaround.

- CSCua69242

  Symptom: In the **show bgp mvpn** command output, the Route Distinguisher Value may be truncated.

  Conditions: This issue occurs in the **show bgp ipv4 mvpn** and **show ip bgp ipv6 mvpn** commands.

  Workaround: There is no workaround.

- CSCua69657

  Symptoms: Traceback is seen when executing the **show clock detail** command.

  Conditions: This symptom is seen when executing the **show clock detail** command with Cisco IOS interim Release 15.3(0.4)T image.

  Workaround: There is no workaround.

- CSCua69725

  Symptom: Pending objects and traffic loss is observed on cell packed interfaces.

  Conditions: This issue occurs when the xxx Router is reload.

  Workaround: Reload the router.

- CSCua70307

  Symptom: When the volume-based lifetime expires, the IPsec session goes down for a few seconds during rekey.

  Conditions: This issue occurs when the user configuration volume-based IPSec lifetime is larger than 100 GB.

  Workaround: Use the default lifetime of 4 GB or any value lesser than100 GB, or disable the volume-based lifetime.

- CSCua70534

  Symptom: Two IS-IS adjacency entries are created with the same SNPA (MAC) address.

  Conditions: Switching the IS-IS process on an existing adjacency interface or misconfiguration could cause two adjacency entries with the same SNPA to be created.

  Workaround: There is no workaround.

- CSCua70593

  Symptom: Shape rate is not enough to allocate the child policy's bandwidth.

  Conditions: Shape rate is not enough to allocate the child policy's bandwidth when the router is loaded with the Cisco IOS 15.3(0.4)T image.

  Workaround: There is no workaround.

- CSCua70906

Symptom: NAT's performance is suboptimal when it is run on ESP100.

Conditions: This issue occurs when you run ESP100 on Cisco IOS XE Release 3.7.0. NAT is not supported on ESP100 that runs on Cisco IOS XE Release 3.7.0.

Workaround: Upgrade to Cisco IOS XE Release 3.7.1 or later.

- CSCua71785

  Symptom: CE2-to-CE1 ping fails after the primary pseudowire is removed and readded with a different VCID.

  Conditions: This happens only if the primary pseudowire is removed from the configuration before the switchover occurs. The ping fails because of traffic black-holing, but is restored back after 300 seconds.

  Workaround: Perform a redundancy switchover to back up the pseudowire before removing the primary pseudowire from the configuration. Also, traffic is automatically restored after 300 seconds.

- CSCua72048

  Symptom: The ESP reloads with a traceback.

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

  Workaround: There is no workaround.

- CSCua74816

  Symptom: Site of Origin (SoO) extended community attributes are seen unexpectedly with the update.

  Conditions: The SoO set statement is set on an outbound route map with a continue clause leading to that route-map clause.

  Workaround: The SoO set statement should not be used on an outbound route map. You should remove it.

- CSCua77720

  Symptom: cpp_svr restart seen on oer border on tunnel flap (external interface) or config replace.

  Conditions: PfR external i/f flapping or MC/BR session flapping.

  Workaround: There is no workaround.

- CSCua77855

  Symptom: Traceback is seen when you unconfigure a router EIGRP.

  Conditions: This is not seen consistently. This behavior varies on different platforms.

  Workaround: There is no workaround.

- CSCua78318

  Symptom: MLPPP fragmentation is not enabled on an MLPPP bundle unless the PPP Multilink Interleave is enabled. This problem does not exist when the PPP Multilink Interleave is enabled.

  Conditions: This issue affects only MLPPP over Serial and does not affect Broadband MLPPP, which does not support MLPPP fragmentation on Cisco ASR 1000 Series Aggregation Services Routers. This problem occurs in Cisco IOS Release 15.1(3)S4 and it was addressed in later releases.

  Workaround: Enable PPP Multilink Interleave on the multilink interface.

- CSCua78779

Symptom: Traceback is seen when the *router ospf <pid>* configuration is removed from the router. The router displays this error message:

```
Jun 27 07:07:45.723 UTC: %SYS-2-CHUNKSIBLINGS: Attempted to destroy  > chunk with
siblings, chunk 549990FC. -Process= "Virtual Exec", ipl= 0,  > pid= 528*.
```

Sometimes, this leads to memory leak when you issue the **no router ospf** command.

Conditions: This issue occurs when you delete the router process when the SPF algorithm is running.

Workaround: There is no workaround.

- CSCua79088

  Symptom: An ESP 80 crash is observed after the Carrier Card is reloaded.

  Conditions: Scaled setup of 7K Xconnects, 3K VPLS, and 4K L2TPV3 circuits.

  Workaround: There is no workaround.

- CSCua79516

  Symptom: SYN packets that are meant to establish FTP data connections are sporadically dropped at the Cisco ASR 1000 Series Aggrrgation Services Routers.

  Conditions: This symptom is observed under the following conditions:

  – the active mode FTP.

  – When you use the PAT.

  Workaround 1: Use the passive mode FTP.

  Workaround 2: Use the static NAT or dynamic NAT configuration.

- CSCua78468

  Symptom: Under a heavy load, L4F may not forward packets to the scan-safe process. Unit may crash while trying to remove scan safe off the interface.

  Conditions: This issue was first identified on a Cisco ISR running the 15.2.4 image.

  Workaround: There is no workaround.

- CSCua78555

  Symptom: Custom protocols does not retain attributes assigned to them using the attribute map after loading the protocol pack. It shows unassigned or other (which is the default for custom protocols).

  Conditions: This symptom is observed when the attributes of the custom protocol are changed using the attribute map and any other protocol pack is loaded.

  Workaround: Reconfigure the attributes for the custom protocols after loading the protocol pack.

- CSCua80204

  Symptom: The EoMPLS remote port shutdown feature does not work.

  Conditions: This symptom is observed if XConnect and a service instance are configured under the same interface.

  Workaround: There is no workaround.

- CSCua80643

  Symptom: The source address of the NTP packet does not change when the routing path changes. The old address is used as the source address.

  Conditions: The issue occurs in Cisco IOS Release 15.2(3)T.

Workaround: Appoint an NTP source or reconfigure the NTP configurations to change the source IP address. However, even if you use the older source IP address as the source IP address, the packets are forwarded based on the RIB table.

- CSCua80659

  Symptom: In the latest mcp_dev image, policy map counters do not get updated for user-defined policies.

  The following **show** commands display a failed example:

```
Router# sh policy-map

Policy Map police-1     Class prec2       bandwidth 12 (%)      police cir 15500000 bc
484375        conform-action transmit         exceed-action drop


Routera# sh class-map

Class Map match-any class-default (id 0)    Match any      Class Map match-all prec2
(id 1)    Match access-group   2002


Router# sh policy-map int

POS8/1/0     Service-policy output: police-1    Counters last updated 00:00:05 ago
Class-map: prec2 (match-all)         9565877 packets, 2429732758 bytes       30 second
offered rate 46539000 bps, drop rate 31055000 bps       Match: access-group 2002
Queueing       queue limit 4650 packets       (queue depth/total drops/no-buffer
drops) 2/0/0       (pkts output/bytes output) 3169279/804996866       bandwidth 12%
(18600 kbps)       police:           cir 15500000 bps, bc 484375 bytes
conformed 3184546 packets, 808874684 bytes; actions:           transmit
exceeded 6381333 packets, 1620858582 bytes; actions:           drop          conformed
0000 bps, exceeded 0000 bps               -----------------> Not updated
Class-map: class-default (match-any)         28697682 packets, 7289203046 bytes
30 second offered rate 139618000 bps, drop rate 6992000 bps      Match: any
queue limit 34100 packets       (queue depth/total drops/no-buffer drops)
34095/1438900/0       (pkts output/bytes output) 27087593/6880240440 RHA_76a#
```

  Conditions: This issue occurs in the conformed and exceeded rates counter, and can be seen after sending the traffic under a customer-defined policy.

- CSCua80784

  Symptom: The number of IP SLAs configurable analysis returns 0.

  Conditions: This issue is seen on devices having free memory of more than 2 GB.

  Workaround: Decrease the IP SLA low-memory value to increase the threshold value.

  Workaround: There is no workaround.

- CSCua81021

  Symptom: ART is accepts the next hop that belongs to its own router.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: There is no workaround.

- CSCua81445

  Symptom: Authenticated status and list of active services are not returned as a part of the COA account-profile-status-query response for the lite session.

  Conditions: This issue occurs whenever COA account query is performed for the lite session.

  Workaround: There is no workaround.

- CSCua82440

Symptom: Records are not exporting out.

Conditions: This symptom is observed after a reload.

Workaround: Change the exporter protocol to V9.

- CSCua83073

  Symptom: The Cisco ASR 1006 Router crashes while running the asr1000rp2-advipservicesk9.03.05.01 .S.152-1.S1.bin image.

  Conditions: This issue occurs only when the RADIUS server receives an invalid attribute from the UID database.

  Workaround: Check the RADIUS attribute retrieved from the UID database. If it is invalid, stop the execution and continue with the uid database operation for the valid radius attribute.

- CSCua83458

  Symptom: Static analysis warnings are seen.

  Conditions: These warnings are observed while publishing REL-11 to the dsgs branch.

  Workaround: There is no workaround.

- CSCua84147

  Symptom: Router crashes during **sh run | format** CLI execution.

  Conditions: This crash is seen only during **sh run | format** execution. All other CLI executions are fine.

  Workaround: Avoid executing **sh run | format**. Instead, execute **sh run**.

- CSCua84879

  Symptom: A crash occurs in slaVideoOperationPrint_ios.

  Conditions: This symptom is observed when the IPSLA video operations are configured andthe **show running-config** command is issued.

  Workaround: There is no workaround.

- CSCua84923

  Symptom: Following a misconfiguration on a two-level hierarchical policy with a user-defined queue limit on a child policy, the UUT fails to attach the QoS policy on the interface even when the correct queuing features are used.

  Conditions: This symptom is observed under the following conditions:

  – The issue must have a user-defined queue limit defined.

  – This error recovery defected is confirmed as a side effect of the C3PL CnH component project due to ppcp/cce infrastructure enhancement.

  Workaround: There is no workaround.

- CSCua84989

  Symptom: Smart Call Home within a VRF is unable to send HTTP requests. The following message is displayed:

  ```
  %CALL_HOME-3-HTTP_REQUEST_FAILED: failed to send HTTP request to:
  https://tools.cisco.com/its/service/oddce/services/DDCEService (ERR 123 : Host name
  resolution failed).
  ```

  Conditions: This issue occurs when the Call-Home is configured with a VRF.

Workaround: Configure a host entry for tools.cisco.com (use dig or nslookup to confirm the IP address <ip host tools.cisco.com n.n.n.n>).

- CSCua85092

  Symptom: RTCP cannot be terminated from the endpoint.

  Conditions: This issue occurs when you configure rtcp-regenerate on the SBC and establish a call between the callers. Use PCMA on both sides and do not trigger transcoding. Transcoding is triggered when a caller sends the reinvite and changes the codec to PCMU.

  Workaround: There is no workaround.

- CSCua85116

  Symptom: Under certain conditions, an ESP may reload and an ESP forced switchover may occur.

  Conditions: This occurs on ESP20 and RP2 with 200 branches, and two BRs each with two exits, and with delay flap on over one of ISP link.

  Workaround: There is no workaround.

- CSCua85239

  Symptom: Flapping BGP sessions are seen if large BGP update messages are sent out and BGP packets are fragmented because midpoint routers have the smaller MTU or IP MTU configured.

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

  – If the midpoint path has an MTU or IP MTU setting that is smaller than the outgoing interface on BGP routers, it will force the BGP router to fragment the BGP packet while sending packets through the outgoing interface.

  – Peering down and the MD5 error do not always occur. They occur only once or twice within 10 tests.

  Workaround: There is no workaround.

- CSCua85934

  Symptom: A session provisioning failure is seen in the ISG-SCE interface. The deactivate or disconnect request has the message authenticator wrongly calculated.

  Conditions: This symptom is observed in the ISG-SCE interface.

  Workaround: There is no workaround.

- CSCua86310

  Symptom: When relay is configured with an unnumbered interface, it appears, the packet is sent out of the loopback interface (instead of the serial interface) to the server, which does not receive the packet.

  Conditions: The issue occurs only when an unnumbered loopback address is used on the relay interface that connects to the server. If an IPv6 address is used directly on the interface, it works fine.

- CSCua87896

  Symptom: QFP exmem is exhausted in the standby FP.

  Conditions: This condition is observed when TCP is used for SIP signalling.

  Workaround: There is no workaround.

- CSCua87944

Symptom: In an IPv6 snooping policy, the keyword **prefix-list** has no effect on the control packet. The keyword only affects binding table recovery. In an **ipv6 nd raguard** policy, the limited-broadcast keyword appears although it is deprecated. It should be hidden and is always on.

Conditions: These symptoms are observed in an IPv6 snooping policy and IPv6 and RA guard policy.

Workaround: There is no workaround.

- CSCua88412

  Symptom: The DNS queries through the Cisco ASR 1000 Series Aggregation Services Router, NAT sessions are not resolved even though the **no ip nat service dns-reset-ttl** command is configured.

  Conditions: This issue occurs if the Cisco ASR 1000 Series Aggregation Services Router configuration includes the **no ip nat service dns-reset-ttl** command.

  Workaround: Remove and add the **no ip nat service dns-reset-ttl** command configuration. Alteratively, if the target platform supports it, reload the ESPs.

- CSCua90577

  Symptom: VRF-aware IP SLAs with ICMP probes fail.

  Conditions: The Cisco ASR 1000 PE Router is configured to send ICMP ping probes to a certain MPLS VPN destination. The ping is received back from the destination, but IP-SLA shows continuous failures. Manual ping via CLI fails as well.

  Workaround: Shut/unshut the ICMP source interface (loopback) or unconfigure and reconfigure the VRF on the loopback interface. However, if the router is reloaded, the issue reappears.

- CSCua91147

  Symptom: ESP 80 crash is observed.

  Conditions: The issue occurs in scaled configurations (7K XConnects, 3K VPLS, 4K L2TPV3 circuits) with FP switchover followed by RP SSO.

  Workaround: There is no workaround.

- CSCua91104

  Symptom: The IS-IS adjacency process shows traceback messaging related to the managed timer.

  Conditions: While configuring ISIS network point-to-point on the LAN interface with ISIS BFD or ISIS IPv6 BFD enabled, traceback does not always ocur; it depends on timing.

  Workaround: Disable ISIS BFD or ISIS IPv6 BFD before issuing **isis network point-to-point** command. Restore ISIS BFD or ISIS IPv6 BFD configuration on LAN interface.

- CSCua91729

  Symptom: BGP assert-enabled images show asserts pointing to bgp_afi2priv_topoid. However, the released images do not have asserts enabled, so these are not seen on the released images.

  Conditions: The topoid access API used to fetch the topoid of IPv6 multicast in BGP needs to be changed. Because the existing API in the code does not use the correct API, the asserts are raised in this DDTS.

  Workaround: There is no workaround. The code should fetch the correct topoid for IPv6 multicast for the VRF.

- CSCua91995

  Symptom: IPv6 IPsec sessions may come up slowly (1 TP per 10 seconds).

  Conditions: This issue occurs when the IPv6 addresses are identical in the first few bytes.

Workaround: There is no workaround.

- CSCua92557

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

  Conditions: This symptom was first identified on Cisco ASR 1000 Series Aggregation Services Routers running Cisco IOS Release 15.1(3)S3 with VASI VRF PAT FW. This issue is seen when the FTP client is on the inside and the active FTP server is on the outside.

  Workaround: Static NAT will work.

- CSCua92741

  Symptom: The allow list prevents the remote neighbors from coming up.

  Conditions: This issue occurs when the remote neighbors are configured with a 32-bit IP address.

  Workaround: There is no workaround.

- CSCua93001

  Symptom: The auto-RP group is not enabled automatically.

  Conditions: The router reboots and starts with the existing configurations.

  Workaround: Manually re-enable **ip pim autorp.**

- CSCua93136

  Symptoms: The switch crashes.

  Conditions: This symptom occurs while sending a DHCPv6 packet with **ipv6 snooping** configured on VLAN configurations.

  Workaround: There is no workaround.

- CSCua93149

  Symptom: Platform kernel messages are displayed on the console.

  Conditions: This occurs when you configure the network-clock synchronization on a Cisco ASR 1002-X platform.

  Workaround: There is no workaround.

- CSCua93635

  Symptom: The xxx router crashes while testing the MPLS-TE features.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: There is no workaround.

- CSCua94117

  Symptom: 1:1 inside local to inside global behavior may be validated.

  Conditions: This symptom is observed under rare timing conditions on Cisco ASR NAT when using the route map (without overload) configuration.

  Workaround: There is no workaround.

- CSCua94563

  Symptom: The traceroute may return * * * instead of host.

  Conditions: This occurs when you move from IPv4 to IPv6 through NAT64 stateful on a Cisco ASR1000 Series Aggregation Services Router.

Workaround: There is no workaround.

- CSCua94947

  Symptom: The RP crashes when downloading the FreeRADIUS Framed-IPv6-Route during MLPPP sessions.

  Conditions: This issue occurs when downloading the FreeRADIUS Framed-IPv6-Route during MLPPP sessions.

  Workaround: There is no workaround.

- CSCua95523

  Symptom: The Cisco ASR1000 Series Aggregation Services Router FP crashes with coredump, causing all the VPN tunnels to halt and possibly renegotiate.

  Conditions: This issue is found to affect DMVPN with IKEv2 setup in a 120-spoke router.

  Workaround: There is no workaround.

- CSCua96209

  Symptom: Fragments get dropped.

  Conditions: This issue occurs when the fragmented traffic is in CGN mode.

  Workaround: There is no workaround.

- CSCua96354

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

  Conditions: This symptom is observed when you issue the following commands:

  show oer master traffic-class performance

  show pfr master traffic-class performance

  Workaround: There is no workaround.

- CSCua96958

  Symptom: In a rarely used configuration of PIC in a confederation, the CEF points the adjacency of the prefix via the repair path instead of an active best path in BGP and RIB.

  Conditions: This occurs when the BGP flags the best path (incorrectly) and repair path (correctly) with recursive-via-connected, even though only the repair path has the gateway that is directly connected to the confederation peer.

  Workaround: Make sure the gateway for the received best path is also directly connected to the CEF to choose the correct outgoing interface. This can be done by setting the next-hop-self feature on the confederation peer from where the best path is received.

- CSCua97282

  Symptom: Router crashes.

  Conditions: No IP routing occurs when router ISIS is running.

  Workaround: Enter the **no ip router isis** command before issuing the **no ip routinger** command to perform IP routing after unconfiguring IS-IS IP.

- CSCua97509

  Symptom: An ESP100 crash is observed.

  Conditions: This issue occurs because of high-scale configurations of VPLS and L2VPN with the traffic. When the ESP switchover is followed by RP SSO, the ESP crashes.

Workaround: There is no workaround.

- CSCua99060

  Symptom: FR back to back.

  Conditions: Reload the box.

  Workaround: shut/no shut the FR interface.

- CSCua99409

  Symptom: ESP reload with an FMAN-FP error.

  Conditions: This issue occurs when you configure the crypto map from the interface when there is a double ACL in the crypto map.

  Workaround: There is no workaround.

- CSCua99969

  Symptom: The IPv6 PIM null register is not sent in a VRF context.

  Conditions: This issue occurs in a VRF context.

  Workaround: There is no workaround.

- CSCub00134

  Symptom: The CPP CP server messages are seen on the CP server logs.

  Conditions: This issue occurs when you check the CP server logs under normal conditions.

  Workaround: This is no workaround.

- CSCub00822

  Symptom: Continuous output of the **show sbc call-stats all current15mins** command.

  Conditions: Adjacencies are more in numbers with running calls.

  Workaround: There is no workaround.

- CSCub01494

  Symptom: AD is not updated to the configured value in the router installed by a client.

  Conditions: When the **ip route** *0.0.0.0 0.0.0.0* **dhcp** *5* is configured, AD is not updated to 5.

  Workaround: There is no workaround.

- CSCub01816

  Symptom: The ESP or CPP of a Cisco ASR 1000 Series Aggregation Services Router crashes with the PfR.

  Conditions: This issue occurs when there are many learn lists.

  Workaround: There is no workaround.

- CSCub02743

  Symptom: The *lfd_install_local_label_for_key:* installation fails on a standby RP.

  Conditions: This issue occurs when you remove the MCPT timer or flap the ATM cell-packed interface.

  Workaround: There is no workaround.

- CSCub04112

  Symptom: The router may lose OSPF routes pointing to the reconfigured OSPF interface.

Conditions: This symptom occurs after a quick removal and readdition of the interface IP address by script or copy and paste.

Workaround: The following are the workarounds:

- Delay entering the commands while removing or adding the IP address. The delay should be longer than the wait interval for LSA origination; by default, it is 500 ms.
- Enter the **clear ip route *** command to refresh the routing table.

- CSCub04345

  Symptom: The Cisco ASR-1002-X Router freezes after four hours in a scaled path jitter SLA probe configuration.

  Conditions: This issue is observed with scaled path jitter SLA probe configuration.

  Workaround: There is no workaround.

- CSCub04740

  Symptom: The Cisco ASR 1000 Series Aggregation Services Router displays the following error message and traceback:

  ```
  SEMAHOG & BADHWUNLOCK.
  ```

  Conditions: This problem occurs when you attach the input marking policy and egress queuing policy to the VP.

  Workaround: There is no workaround.

- CSCub05559

  Symptom: On 1RU, the bootflash (eUSB) gets disconnected rarely after booting the system. As a result, the system reboots, but cannot stay up without eUSB storage.

  Conditions: This issue occurs randomly, and there is no specific pattern that can be mentioned.

  Workaround: There is no workaround.

- CSCub05643

  Symptom: When you change the interface name in the **aaa group server radius rad123 ip radius source-interface** <*interface name*> command, the changes do not take effect on the source interface of the RADIUS packet.

  Conditions: When the configured RADIUS source interface is changed, the new interface does not take effect immediately.

  Workaround: Reload the router, unconfigure the router, and then reconfigure the server group.

- CSCub06131

  Symptoms: The IPSLA sender box is reloaded with the following message:

  ```
  SYS-6-STACKLOW: Stack for process IP SLAs XOS Event Processor running low, 0/6000
  ```

  Conditions: This issue is observed in the IPSLA sender box.

  Workaround: There is no workaround.

- CSCub06859

  Symptom: OSPFv2 NSR on quad-sup VSS does not work. The router stops sending hello packets after switchover.

  Conditions: This issue is observed on quad-sup VSS with OSPFv2 NSR.

  Workaround: Clear the IP OSPF process after NSR switchover.

- CSCub07430

Symptom: ICMP Echo reply with the wrong src IP address from the Cisco ASR 1000 router.

Conditions: The issue occurs when the MPLS Multi-VRF Selection is configured with PBR.

Workaround: There is no workaround.

- CSCub07679

  Symptom: The router may crash or generate datapath trace-back.

  Conditions: This symptom is observed when one of the following conditions is met:

  – MMON is enabled.

  – The NBAR is enabled and configured to look into IPv6 tunnels, using one or both the following CLI commands:

  a. **ip nbar classification tunneled-traffic ipv6inip**

  b. **ip nbar classification tunneled-traffic teredo**

  Workaround: Perform the following steps for the conditions described previously:

  – Disable media monitoring.

  – Disable NBAR classification of tunneled trafficby using the **# no ip nbar classification tunneled-traffic ipv6inip** command and the **# no ip nbar classification tunneled-traffic teredo** command respectively.

- CSCub07695

  Symptom: The VRRP IP address owner scenario can be triggered by matching a vIP with the IP of a different physical interface.

  Conditions: This issue occurs when the VRRP is incorrectly configured to have a primary vIP that is equal to another interface's physical IP address.

  Workaround: Configure the VRRP to have a vIP within the same subnet of the interface on which it is present.

- CSCub07855

  Symptom: A VRF error message is displayed in the router.

  Conditions: This symptom occurs during router bootup.

  Workaround: There is no workaround.

- CSCub08714

  Symptom: Poor performance is seen for multicast on Cisco ASR 1000 Series Aggregation Services Routers over DMVPN.

  Conditions: This symptom occurs under both the following conditions:

  – Multicast packets should come in via tunnel interface (not a physical interface).

  – The negate signaling (NS) flag has to be set on one of the interfaces in the MFIB (S,G) entry.

    If both these conditions are met, the packet is punted to the control plane and forwarded in software in addition to the hardware forwarding, thus causing duplicates. Note that the NS punts are periodic/throttled, and not all multicast packets are punted because of NS. Thus, the duplication is intermittent/periodic.

  Workaround: There is no workaround.

- CSCub09124

  Symptom: The MDT tunnel goes down.

Conditions: This symptom is seen in MVPN. If the **ip multicast boundary** command on the noncurrent RPF interface blocks the MDT group, it may cause MDT tunnel failure.

Workaround: Adding the **static join** command in the PE loopback interface may help you work around the problem temporarily.

- CSCub10102

  Symptom: The PCMCIA flash card formatting error occurs on the Cisco UBR7200-NPE-G1.

  Conditions: This issue occurs after swapping different characteristics, such as size, clusters, or sectors, of the compact flash card on Cisco UBR7200-NPE-G1.

  Workaround: Reload Cisco UBR7200-NPE-G1.

- CSCub10951

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

  Conditions: This symptom is observed under the following conditions:

  1. The following configuration exists at all RRs that are fully meshed:
  – bgp additional-paths select best-external
  – nei x advertise best-external
  2. For example, RR5 is the UUT. At UUT, there is,
  – Overall best path via RR1.
  – Best-external (best-internal) path via PE6 (client of RR5): for example, the path is called "ic_path_rr5".
  – Initially, RR5 advertises "ic_path_rr5" to its nonclient iBGP peers, that is, RR1 and RR3.
  3. At PE6, unconfigure the route so that RR5 no longer has any inter-cluster BE path. RR5 sends the withdrawals to RR1 and RR3 correctly.
  4. At PE6, reconfigure the route so that RR5 will have "ic_path_rr5" as its "best-external (internal) path." At this point, even though the BGP table at RR5 gets updated correctly, it does not send the updates to RR1 and RR3. They never relearn the route.

  Workaround: Hard/soft clear.

- CSCub12361

  Symptom: When a neighbor that is not created is configured to an existing peer group, a memory leak of 1 KB is triggered along with the following error message:

  ```
  Members of peer-group must use the same transport.
  ```

  Each time a similar command is entered, a new memory leak of the same size occurs. Therefore, this issue is not surface-impacting.

  Conditions: This issue occurs when you execute the **neighbor <i***p-address***> peer-group <***peer-group name***>** command in the router configuration mode, where the peer group name is valid and configured. However, the neighbor is not created. For example, create a peer group *neighbor rrc peer-group* and add an IPv4 neighbor to the peer group. When you configure the peer group to IPv4 *nei 51.3.3.2 peer-group rrc* and add an IPv6 neighbor to the same peer group to trigger a transport error *nei 5133::2 peer-group rrc Error*, members of the peer group must all use the same transport. Check for memory leak *do show mem deb leak.* This will produce an entry for a newly generated memory leak.

  Workaround: Avoid misconfigurations since the effect of .. is a localized memory leak.

- CSCub13697

Symptom: The embedded IP addresses in the SIP packets may not get translated as expected.

Conditions: This was first identified on a Cisco ASR 1000 Series Aggregation Services Router running the Cisco IOS 15.1(3)S3 image. The softswitch inside ... was configured with static PAT for TCP and UDP port 5060 to a mapped IP address, A. The same softswitch on the inside of ... was configured with bridged media, and the Cisco ASR 1000 Series Aggregation Services Router was configured with dynamic PAT overload to a mapped address, B. Also, the inbound and outbound connections were configured to use different mapped IP addresses.

Workaround: Use the static 1-1 NAT for the softswitch on the inside of ....

- CSCub13983

  Symptom: There are two calls to mcp-sysinit.

  Conditions: This is seen frequently.

  Workaround: There is no workaround.

- CSCub14299

  Symptom: The router reloads when no mediatrace initiator is issued.

  Conditions: This issue occurs when traceroute is enabled for a mediatrace session.

  Workaround: Disable traceroute under each configured mediatrace session.

- CSCub15542

  Symptom: The IOSD restarts.

  Conditions: This issue occurs when configuring MPLS LSP trace.

  Workaround: There is no workaround.

- CSCub16403

  Symptom: Timestamps are displayed as per the local wall clock time.

  Conditions: This problem occurs when the **show flow monitor MON cache** command is issued on the Cisco ASR 1000 Series Aggregation Services Routers running the Flexible Netflow feature.

  Workaround: There is no workaround.

- CSCub16463

  Symptom: The **bandwidth remaining ratio** command does not accept **atm** keyword for an ATM cell tax compensation.

  Conditions: This issue occurs during the basic command-line configuration.

  Workaround: Use the bandwidth remaining percent configuration instead of bandwidth remaining ratio.

- CSCub17584

  Symptom: IOSD crashes are seen in Cisco ASR 1000 Series Aggregation Services Router MVPN sessions. When the sessions are cleared, all the IGMP joins are released, and the sessions are brought up. When about 400 to 500 IGMP join, a crash occurs.

  Conditions: A crash is observed when clearing the ASR 1000 Series Aggregation Services Router MVPN sessions on LAC using the **clear pppoe all** command.

  Workaround: There is no workaround.

- CSCub17585

  Symptom: The system crashes and reboots with AVC1.0.

Conditions: FNF collecting HTTP fields such as host, with AVC1.0. The crash occurs infrequently in context with MSN traffic.

Workaround: Removing the HTTP fields from the FNF records will eliminate the problem.

- CSCub17852

  Symptom: Improper accounting attributes are received as part of the COA account query response for lite session.

  Conditions: This issue occurs whenever COA account query is performed for a lite session.

  Workaround: There is no workaround.

- CSCub17985

  Symptom: A memory leak is seen when IPv6 routes are applied on the per-user sessions.

  Conditions: This symptom is seen if IPv6 routes are downloaded as part of a subscriber profile. On applying these routes to the sessions, a memory leak is observed.

  Workaround: There is no workaround.

- CSCub18236

  Symptom: The ES, ES20, and SIP-200 line cards crash when **no shutdown** command is executed in the tunnel interface.

  Conditions: This issue occurs when you attach to the line card and execute the **shut** and **no shutdown** commands on the tunnel interface.

  Workaround: Execute the **no shutdown** command only for the tunnel from the RP.

- CSCub18243

  Symptom: When the traffic is matched with the last statement of an ACL, the performance of the IPv6 traffic is impacted more than that of the IPv4 traffic.

  Conditions: This issue occurs when an ACL with more than 20 entries and high traffic rate, hits one of the last statements of the ACL.

  Workaround: There is no workaround.

- CSCub18741

  Symptom: Fragmented SIP packets may get dropped due to FirewallInvalidZone.

  Conditions: NAT and Firewall configured in VASI interface, SIP payload needs to be translated and the length of translated ip address is different from the prenat address or PAT is configured.

  Workaround: There is no workaround.

- CSCub18786

  Symptom: When the Feature Navigator for the Cisco ASR1001 Router is run for universalk9_npe image and adventerprise image, the same features, that is, they should be in sync and no extra features should be displayed.

  Conditions: It is a day 1 issue, and consistently reproducible.

  Workaround: There is no workaround.

- CSCub19921

Symptom: Route flaps may occur after a switchover when a router is configured to use ISIS IETF NSF. The route timestamp is refreshed in the **show ip route** command output. Packet traffic may also be dropped as a result of the switchover. Occurs with point-to-point interface or on a LAN configured as point-to-point.

Conditions: Configure ISIS NSF IETF and the point-to-point interface.

Workaround: There is no workaround.

- CSCub20516

  Symptom: The section output modifier does not work correctly for a specific sequence of commands when the parser command serializer is enabled.

  Conditions: This issue occurs when you use the hardware and configuration similar to that of NTT. Invoking the **show policy-map control-plane** section CoPP_PPPoE will produce the preconditions that are necessary to affect the subsequent invocation of **show interfaces Port-channel**1 *Etherchannel* | section IDBs. This produces incorrect output during the execution.

  Workaround: Repeat the failed command twice.

- CSCub20803

  Symptom: The EIGRP delay value cannot be calculated correctly.

  Condition: This issue occurs when the nonwide metric router receives prefix from the widemetric router.

  Workaround: Use the widemetric routers for both the receiver and the sender.

- CSCub21340

  Symptom: A segmentation fault occurs and the router reloads continuously.

  Conditions: The issue occurs when the router is reloaded with CFM over an XConnect scale configuration.

  Workaround: There is no workaround.

- CSCub23298

  Symptom: The multicast traffic over a PVC bundle always go to prec 0 pvc.

  Conditions: Multicast over PVC bundle is configured.

  Workaround: There is no workaround.

- CSCub24410

  Symptom: In a scaled OTV setup (with 50 overlays and 2000 EFP configurations), when one ED fails in a multihomed site, the remote ED has two next hops in MLRIB for the same MAC address.

  Conditions: This issue occurs when you have a multihomed setup in one site and one ED in another site, configure 50 overlays with 40 EFPs per overlay, send end-to-end traffic, and bring down one ED in the multihomed site. The third ED will have MAC addresses with two next hops in the MLRIB in some BDs.

  Workaround: There is no workaround.

- CSCub25280

  Symptom: The same inside global address is assigned to multiple inside local addresses in the dynamic route map configuration and ALG traffic.

  Conditions: This issue occurs in the ALG traffic dynamic route map configuration.

  Workaround: Use static or dynamic NAT configuration without route maps.

- CSCub25362

  Symptom: A crash occurs when reloading a Cisco ASR 1000 Series Aggregation Services Router RP2 with multicast configuration.

  Conditions: This symptom is observed on rp2 XE3.8 mcp-dev nightly image when you reload the router with the attached configuration.

  Workaround: There is no workaround.

- CSCub25419

  Symptom: A Cisco ASR1000 Series Aggregation Services Router ESP may crash at pfr_tt_ll_resp_cb when you introduce delay and flapping for TC. That is, **clear pfr master border *** on MC.

  Conditions: Running PfR DMVPN setup with scaled number of branches, and **clear pfr master border *** on MC.

  Workaround: No PfR session flapping.

- CSCub26079

  Symptom: Service policies are not applied on the ATM interface.

  Conditions: This issue occurs in the following scenarios:

  – The client is configured with PPP CHAP hostname peer.

  – A PPPoA session is established and policies 7up, and sprite are installed on the interface of UUT.

  – PPP CHAP hostname rate is configured on the client later.

  – The time policies are downloaded from RADIUS that have not replaced with the previous policies 7up and sprite values.

  Workaround: There is no workaround.

- CSCub26441

  Symptom: A Cisco ASR1000 Series Aggregation Services Router with ESP100 crashes if the out-of-range queue ID QID is included while issuing **mcp_bb_99#sho plat hard qfp act inf bqs sch qid <*qid*>** command. As a result, ESP100 will dump a core and reload, potentially impacting traffic.

  Conditions: A Cisco ASR1000 Series Aggregation Services Router must have one or more redundant ESP100s operating, and the **sho plat hard qfp act inf bqs sch qid <*qid*>** command issued with an out-of-range QID. Under normal circumstances (when other ESP models other than ESP100 are present), the following message displayed for a bad QID:

  ```
  % Error: Failed to gather BQS information for QID 0xc03, QID out of supported range.
  ```

  Workaround: Ensure that you include a correct QID. there is no work-around if the fix is not present.

- CSCub26822

  Symptom: When the prefix has multiple paths from the same next hop, one of these paths become the best path. Another path from a different next hop is computed for RR best external path to advertise to the peers that are configured to receive this path. The RR best external path advertised to the BGP peers may not be withdrawn when the source withdraws this path from the UUT. This may happen when the UUT BGP table has multiple paths that are the same next hop as the best path.

Conditions: This issue occurs when there are multiple paths from the same next hop in the PCP table and an RR best external path having a different next hop. When this RR best external path is withdrawn, the path is still seen in the peer that received it. The RR does not withdraw this route from the peers.

Workaround: Use the **clear ip bgp** <*peer*> command to resend the prefixes to the peer. Alternatively, use the Enhanced Route Refresh feature to avoid this issue.

- CSCub27029

  Symptom: In extremely rare cases, the **sh ip nat trans** command may cause an error message to be displayed or a crash to occur.

  Conditions: This occurs rarely.

  Workaround: Downgrading to a release prior to Cisco XE 3.6.0 is a possible workaround. A fix is expected, starting with Cisco IOS XE Release 3.7.1.

- CSCub27590

  Symptom: The RP crashes during the EXEC process.

  Conditions: This issue occurs when you remove or readd the BGP AD L2 VFI with debug enabled.

  Workaround: There is no workaround.

- CSCub27178

  Symptom: The long-term service gets stuck in an attempting state and does not get established.

  Conditions: This condition occurs during the following scenarios:

  – When the Cisco ISG session restart events are configured, service is stuck in the attempting state, or there is an IP address mismatch.

  – When the session churning through idle timeout or session timeout is configured.

  Workaround: GGSN retains the allocated IP address for a user (tagged by IMSI for GTP) within the configured timer window. Essentially, after the first PDP context is deleted and the second one arrives, GGSN allocates the same IP address for the user within the hold time. This is achieved without the need to specify the address in End User Application - Information Element (EUA-IE) from the iWAG in the CPC. The iWAG will not maintain any binding by itself; this is GGSN's responsibility. Administrators should configure the iWAG so that the per-APN DHCP lease time matches the hold-time value. The following is a sample configuration of a session restart event:

```
class-map type traffic match-any TC_OPENGARDEN
match access-group output name ACL_OUT_OPENGARDEN
match access-group input name ACL_IN_OPENGARDEN
!
policy-map type service OPENGARDEN_SERVICE
20 class type traffic TC_OPENGARDEN
accounting aaa list PROXY_TO_CAR
!
class type traffic default in-out
drop
!
!
policy-map type control BB_PROFILE
class type control always event session-start
10 service-policy type service name OPENGARDEN_SERVICE
20 authorize aaa list ISG_PROXY_LIST password cisco identifier mac-address
!
class type control always event session-restart
2 authorize identifier mac-address
4 set-timer IP_UNAUTH_TIMER 4
```

- CSCub29610

  Symptom: The Qos MIB filter statistics do not add up to the same number as the QoS MIB class statistics.

  Conditions: This issue occurs on a Cisco 7600 Router running the IOS XE 3.7 code. This does not impact the Cisco ASR 1000 Series Aggregation Services Router and the Cisco ASR 903 Router.

  Workaround: Avoid modifying the filters in the class map. If you need to modify, delete the class-map and configure a new class-map with the desired filters.

- CSCub29733

  Symptom: The NAT HA feature is not going into PI20 because performance degradation issues were found with the CEF changes made for this feature.

  Conditions: Any changes that we checked into resiliency@dev4 for the NAT HA feature needs to be backed out. Once that is done, we need to uprev latest of dev4 (without changes made for NAT) to 15.3(1)T/PI20.

  Workaround: There is no workaround.

- CSCub30577

  Symptom: Unexpected RTs are attached to redistributed routes in a VRF.

  Conditions: This issue occurs when the export map for a VRF contains a clause that sets both the RT matches a match as-path clause. In such a scenario, the match as-path clause will automatically match, causing the attachment to occur.

  Workaround: There is no workaround.

- CSCub31399

  Symptom: The DHCPv6 client gives a parse error while receiving the *NOPREFIX-AVAIL* from the server.

  Conditions: This issue occurs when the status code is NOPREFIX-AVAIL for the client REQUEST.

  Workaround: There is no workaround.

- CSCub31477

  Symptom: A Cisco ISG router configured for Layer 2 Connected Subscriber Sessions does not respond to ARP replies after a subscriber's ARP cache has expired.

  Conditions: This symptom occurs when the router is configured as ISG L2-Connect, the router has configured HSRP as the high-availability method, and the subscriber-facing interface is configured with the **no ip proxy arp** command. This issue is not seen if either HSRP is removed or the **ip proxy arp** command is enabled.

  Workaround: Clear the subscriber session. After the subscriber is reintroduced, the issue is resolved. You can also configure **ip proxy arp** on the HSRP-configured interface.

- CSCub32500

  Symptoms: The router crashes in the EIGRP mode.

  Conditions: This symptom is observed on the EIGRP flaps.

  Workaround: There is no workaround.

- CSCub32890

  Symptom: A request to include the max support user-queue information for the output of the **sh platform hardware qfp active infrastructure bqs capabilities** command is displayed.

  Conditions The current **show bqs capability** command output does not include this information.

Workaround: There is no workaround.

- CSCub33119

  Symptom: The **?sh pl software interface fp active name interfacexxx ip reassembly?** command does not display the reassembly parameter correctly.

  Conditions: When the router is not configured with the reassembly max-reassembly value, it uses the default value, 16. In this scenario, the output of the **sh ip reassembly gigabitEthernet 0/0/0** command will display reassembly value correctly, but the binos **show platform software inter fp active name xxx ip reassembly** command will not display the value correctly.

  Workaround: There is no workaround.

- CSCub33602

  Symptom: An IGMP query with the source IP address 0.0.0.0 triggers a querier election process. As a consequence, the port on which this packet is received is marked as the mrouter port for that VLAN.

  Conditions: This issue occurs when an IGMP query with source IP address 0.0.0.0 is received.

  Workaround: Configure an ACL to block packets with the source IP address 0.0.0.0 and apply it to the relevant interfaces.

- CSCub33877

  Symptom: During issue loadversion, when downgrading from Texel (or later) to YAP (v151_1_sg_throttle or earlier), the standby RP keeps reloading due to the out-of-sync configuration.

  Conditions: This symptom occurs during the issue loadversion operation. The newer version of the image supports IPv6 multicast, while the older version of image does not.

  Workaround: There is no workaround.

- CSCub34128

  Symptom: Ucode crash occurs followed by an FP crash seen on sending GTP traffic.

  Conditions: This issue occurs when traffic is sent from the SGPRS simulator.

  Workaround: There is no workaround.

- CSCub34756

  Symptom: An RP crash is observed.

  Conditions: When an RP card is hosting the TP tunnel midpoint, the RP crashes during the SSO operation.

  Workaround: There is no workaround.

- CSCub35526

  Symptom: The output of the **plim qos input queue** command reflects on all interfaces of the same SPA.

  Conditions: When configured **plim qos input queue** for a interface, the configuration reflects all the interfaces on the SPA.

  Workaround: There is no workaround.

- CSCub36301

  Symptom: The BFD sessions crash when the FP is switched over.

Conditions: This occurs when the peer is Cisco ASR1000 RP1 with large BFD sessions.

Workaround: There is no workaround.

- CSCub38174

  Symptom: Memory leak is seen on the standby RP.

  Conditions: This issue occurs only on the standby card in which the ERP interface is in the down state. Ideally, the platform should not punt packet to the ERP process when the interface is down. Also, the ERP should drop and free the memory for punted packet.

  Workaround: There is no workaround.

- CSCub38559

  Symptom: When static recursive routes are used in an MVPNv6 environment, multicast traffic loss may occur due to a failure in determining the correct RPF interface for a multicast source or rendezvous point.

  Conditions: This issue occurs if a static route to an IPv6 address at a remote site of a VPN cloud resolves via a BGP route, resulting in a failure to install the required MDT alternate next hop in the recursively referenced BGP route.

  Workaround: Execute the **show ipv6 rpf vrf X <***address***>** command for the address within the recursively referenced BGP prefix range to install the required alternate next hop.

- CSCub39131

  Symptom: Packets get dropped.

  Conditions: 5cps basic sip call.

  Workaround: Reduce the traffic load from 5 cps to 2 cps.

- CSCub43292

  Symptom: The device displays an error while using the built-in environment variable of the Identity Event detector applet called "$_interface.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: The actual variable is "$_identity_interface" and not "$_interface", which stores the value of the interface.

- CSCub44215

  Symptom: In the routed VPLss scenario, when BDI interface on a Cisco ASR 1002 router is configured in VRF and receive packets on VPLs, the VFI (from a PE router with XConnect) meant for the VPN prefixes imported via route-target import from its l3vpn mpbgp peer (another PE). This corrupts the packets. The destination device drops all the packets as it contains IP option.

  Conditions: This issue occurs only for the destination learned via the route target import policy. The devices behind the PE (having scanned) can ping the BDI interface, and the routes are directly connected to a Cisco ASR 1000 Series Aggregation Services Router or learned via another device in the same VRF. This issue is seen in the 15.2(2)S1 and 152-4.S.bin images.

  Workaround: There is no workaround.

- CSCub46570

  Symptom: The image cannot be built with an undefined symbol.

  Conditions: The commit error triggers the compiling issue.

  Workaround: There is no workaround.

- CSCbuub47374

  Symptom: The router crashes during the IP SLA probe.

  Conditions: This issue occurs during the IP SLAs removal and reconfiguration.

  Workaround: There is no workaround.

- CSCub48495

  Symptom: The router crashes when it runs the RT constrain feature and also, have redistribute connected or network statements in other address-families with route-map.

  Condition: This issue occurs when the route map is removed and then the RT filters are added.

  Workaround: There is no workaround.

- CSCub50946

  Symptom: The bandwidth value is not correctly cloned to the virtual-access interface of the virtual template interface. When a FlexVPN client connects to the IOS head-end and the virtual template does not have bandwidth configuration, the FlexVPN client uses the default value of 100 KB.

  Conditions: This issue occurs when the FlexVPN server runs on a Cisco IOS15.1(3)T or later image. The client connects and the virtual access interface gets cloned with the correct bandwidth (100 KB). When the client disconnects, and then reconnects, the bandwidth of the new virtual access interface will be 10000 KB.

  Workaround: Manually configure a nondefault bandwidth on the virtual template interface.

- CSCub51087

  Symptom: ODR is not working.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: There is no workaround.

- CSCub51279

  Symptom: A Cisco ASR 1000 Series Aggregation Services Router resets its FP a with FW NAT feature combination.

  Conditions: A Cisco ASR 1000 Series Aggregation Services Router resets its FP with a FW NAT feature combination along with traffic.

  Workaround: There is no workaround.

- CSCub51527

  Symptom: The line card crashes during switchover.

  Conditions: During switchover, when the Tableid HA of the line card tries to open an IPC port of the new active RP, the port is not created and the line card crashes.

  Workaround: There is no workaround.

- CSCub52339

  Symptom: A Cisco router that runs the Performance Routing (PfR) Master Controller function may reload unexpectedly after the **shutdown** command is executed under PfR master.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: Do not execute the **shutdown** command on the router.

- CSCub52639

  Symptom: The embedded IP addresses in the SIP packets are not translated.

Conditions: This issue occurs when different NAT mappings translate to the same IP address in the header and payload.

Workaround: Use the same configuration for both header and embedded translation for the same IP address.

- CSCub53087

  Symptom: A high number of GTPv0 and GTPv1 packet drops with GTP permit-error OFF. On ASA, this feature can be turned ON.

  Conditions: This issue occurs when a zone-based firewall is configured for the GTP traffic and GTP permit-error is OFF.

  Workaround: There is no workaround.

- CSCub53660

  Symptom: A stale multicast alternative route for the tunnel route is found after the level-1 interarea tunnel route is replaced by a nontunnel level-2 route.

  Conditions: When multi-cast intact is enabled and shut/unshut an interface causes topology change only in level-2. The result of the level-2 SPF changes, but the level-1 topology and level-1 SPF result does not change. Thus, the stale multicast alternative route for the level-1 tunnel route is not deleted even though the tunnel route is replaced by a level-2 nontunnel route.

  Workaround: Change the interface circuit type to level-1-2 or adjust the ISIS topology in such a way that the tunnel route is replaced by a nontunnel route of the same level.

- CSCub54686

  Symptom: When the ultra kernel is crashes, the kernel core is not dumped.

  Conditions: This issue occurs when the ultra kernel crashes.

  Workaround: There is no workaround.

- CSCub54872

  Symptom: When 32 prefixes are applied to an interface, for example a loopback, is not being treated as connected. This can impact the connectivity of the 32-bit prefix.

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

  Workaround: Use a shorter prefix.

- CSCub54993

  Symptom: When attaching an interface to a downstream VRF, the following warning message may be displayed even if the VRF in question does not have the IPv6 address family configured:

  ```
  % IPv6 does not support hdvrf interface Ethernet0/0
  ```

  Conditions: This error message is displayed only when a downstream (half-duplex) VRF is configured on an interface, and that VRF was created using the **vrf definition** command.

  Workaround: This message is a reminder to indicate that IPv6 does not support half-duplex VRFs and that VRF forwarding configuration will be ignored for the IPv6 address family.

- CSCub55036

  Symptom: A combination of static NAT and Firewall allows the flow of ICMP timestamp even though the user-defined ACL is dropped.

  Conditions: NAT with Firewall for ICMP timestamp flow

  Workaround: Apply an ACL on the interface to deny ICMP time-stamp request.

- CSCub55948

  Symptom: The Cisco ASR 1000 Series Aggregation Services Routers contain a vulnerability that could allow an unauthenticated attacker on an adjacent network segment to cause a Denial of Service (DoS) and reload the box. A Cisco ASR 1000 router, that is configured for bridge domain interface (BDI) routing, may crash.

  Conditions:A Cisco ASR 1000 Series Aggregation Services Router that is configured for BDI routing, may crash if it receives crafted fragmented ICMP packets that are meant for L2 broadcast or multicast addresses.

  Workaround: Under the interface BDI, use access-list to deny the ICMP packets meant for the subnet broadcast address.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores at the time of evaluation were 6.1/5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-5723 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCub56946

  Symptom: 100 percent traffic loss is seen in all the VCs.

  Conditions: Flap the MST (special PW) instance.

  Workaround: It recovers by itself after 5 minutes.

- CSCub57735

  Symptom: ip nat inside source route-map NAT-MAP pool xyz force cannot be removed and shows that dynamic NAT is in use even when there are no NAT entries.

  Conditions: 1) Configure dynamic NAT 2) Relay SIP traffic, which hits NAT entries 3) Stop the test, clear NAT entries, and remove the CLI.

  Workaround: Use the **no ip nat inside source route-map NAT-MAP pool xyz force** command instead.

- CSCub58238

  Symptom: The FP crashes when the ATM VC bundle configuration is loaded.

  Conditions: The issue is seen in configurations of around 200 ATM VC bundles.

  Workaround: The FP will be stable after the initial crash.

- CSCub58483

  Symptom: The **line radius-server attribute** *6* **on-for-login-auth** command can no longer be configured on images where CSCtu18661 has been integrated.

  Conditions: Use CSCtu18661 integrated in an image.

  Workaround: There is no workaround.

- CSCub58490

  Symptom: A memory leak occurs on the standby RP due to the **banner** command.

  Conditions: This issue occurs when the **banner** command is available in the active running configuration.

  Workaround: Prior to booting up the standby server, remove the **banner** command from the active running configuration.

- CSCub58775

  Symptom: A crash may occur in the standby RP of a Cisco ASR 1000 Series Aggregation Services Router.

  Conditions: This issue may occur after an OIR of a power supply and probably other similar events.

  Workaround: There is no workaround.

- CSCub58991

  Symptom: The **show ppp multilink** command does not display the correct configuration status for MLPPP Fragmentation, Interleaving, and Distributed MLPPP platform status. The Cisco ASR1000 was enabling Multilink PPP fragmentation (legacy mode) enabled by default. Fragmentation should Series Aggregation Services Routers be enabled only if configured on the multilink bundle interface or Virtual-Template (Broadband MLPPP).

  Conditions: This issue is seen on all the multilink PPP configurations.

  Workaround: There is no workaround.

- CSCub59275

  Symptom: The configuration of the CT3 controller serial interface s does not match between and standby RPs. Error messages such as `%COMMON_FIB-4-FIBHWIDBMISMATCH: Mis-match between hwidb Serial1/0/1/2:0 (ifindex 634)` and `fibhwidb Serial1/0/1/1:1 (ifindex 634)` appear on the standby RP during controller configuration. IP addresses are assigned to wrong serial interfaces. When RP switchover occurs, traffic does not pass due to the mismatch.

  Conditions: This issue occurs when configuring the CT3 SPA in a dual RP router.

  Workaround: There is no workaround.

- CSCub59493

  Symptom: The CPU remains at 100 percent after the SNMPv2c walk even after 5 minutes.

  Conditions: This issue occurs when an SNMP walk is performed on the MPLS-LSR-STD MIB.

  Workaround: There is no workaround.

- CSCub60278

  Symptom: The OSPF neighbor cannot enable over point-to-multipoint ATM bundles .

  Conditions: This issue occurs when two ASR1000 Series Aggregation Services Routers are directly connected with ATM PVC bundles and one end is a point-to-point subinterface and the other is a remote multipoint subinterface. Try to execute the ospf over bundle.

  Workaround: Change the interface to P2P ATM.

- CSCub62988

  Symptoms: Consecutive crashes occur.

  Conditions: This symptom is observed in an ASR 1000 Series Aggregation Services Router with ESP10, and Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCub63440

  Symptom: An EEM applet may execute its action statements twice.

  Conditions: This issue is seen when the configured event in the EEM applet is a cron timer requiring the NTP to be configured on the system.

  Workaround: There is no workaround.

- CSCub65151

  Symptom: The CCP of the Cisco ASR 1000 Series Aggregation Services Routers crashes when the core-facing MPLS interface on the NPE is hutdown.

  Conditions: This symptom occurs rarely.

  Workaround: There is no workaround.

- CSCub65293

  Symptom: The VSAs actual-data-rate-upstream and actual-data-rate-downstream are duplicated in the access request sent bya Cisco ASR 1000 Series Aggregation Services Router.

  Conditions: This issue occurs when the ANCP port is configured under a subinterface or ATM VC, and the ANCP, port is in the UP state and Established.

  Workaround: There is no workaround.

- CSCub66311

  Symptom: After NSR switchover, Cisco IOS router do not listen for the DR multicast address on the interface.Before switchover: show iplipv6 int Multicast reserved groups joined: 224.0.0.5 224.0.0.6 Joined group address(es): FF02::1 FF02::2 FF02::5 FF02::6 After switchover: Multicast reserved groups joined: 224.0.0.5 Joined group address(es): FF02::1 FF02::2 FF02::5

  Conditions: NSR OSPF switchover.

  Workaround: Execute either the **shut** interface command or the **no shut interface** command.

- CSCub66569

  Symptom: The Cisco ASR1000 Series Aggregation Services Routers generate IGMP packets all of which have a zero source MAC address.

  Conditions: This random issue occurs when the OTV ED/Bridge-domain is configured.

  Workaround: There is no workaround.

- CSCub66957

  Symptoms: In a basic LSM setup of PE-P-PE where the router is performing a disposition function, the ESP40 may crash.

  Conditions: The ESP40 may crash the moment traffic hits the box.

  Workaround: Execute the following commands to disable LRE:

  - **set plat hard qfp active feature multicast v4 lre off**
  - **set plat hard qfp active feature multicast v6 lre off**

- CSCub66524

  Symptom: Reload may occur.

  Conditions: On a Cisco ASR 1000 Series Aggregation Router NAT, a reload may occur depending on the timing condition in the out2in particular invalid packets.

  Workaround: There is no workaround.

- CSCub67101

  Symptom: The POS interface line protocol goes down with encapsulation PPP in an MPLS setup.

  Conditions: This symptom occurs when configuring encapsulation PPP on both ends of PE1 and CE1, and then configuring XConnect in the customer-facing interface of PE1.

  Workaround: Reconfigure the XConnect settings.

- CSCub68021

  Symptom: The **show interface** command on a SPA interface shows "0" for "unknown protocol drops". Yet when the same interface is polled for ifInUnknownProtocols, a value is returned.

  Conditions: This issue occurs when there are normal polling events.

  Workaround: There is no workaround.

- CSCub68200

  Symptom: The FP may crash while flapping sessions with the ISG services or flapping the ISG services themselves.

  Conditions: This behavior may be seen on the Cisco ASR 1000 Series Aggregation Services Routers running Release 15.1(2)S or later release images. The ISG services that are involved are Traffic Class services, and they may have any of the L4R, DRL/Policing, or accounting-based features applied. This issue may be seen when such services are quickly added and removed from a subscriber.

  Workaround: There is no workaround.

- CSCub69350

  Symptom: When using the **radius-server domain-stripping** command, the aaa accounting suppress null-username' command does not work. The router sends a null username in the accounting packet even when the command is issued.

  Conditions: This issue occurs when you use the **radius-server domain-stripping** command and the **use aaa accounting suppress null-username** command.

  Workaround: There is no workaround.

- CSCub69414

  Symptom: A traceback occurs in FreeUInt64 on booting up router.

  Conditions: This issue occurs when tracebacks are seen when a Cisco ASR1006 Router boots up.

  Workaround: Traceback occurs are because of the **snmp-server enable traps entity-qfp mem-res-thresh** command. Disable the **snmp-server enable traps entity-qfp mem-res-thresh** command.

- CSCub69764

  Symptom: Occasionally, after full chassis reload, all ATM autovc fail to come up when PADI is received the CPE does not gets PADO. All the PPPoEoA sessions fail to establish on the chassis.

  Conditions: The trigger for this issue is unknown. This occurs intermittently, for example, after full chassis reload, once every ~50 reloads.

  Workaround: Reload the chassis again.

- CSCub70239

  Symptom: Customers see the following error messages repeatedly:

  - `%IOSXE-3-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:109 TS:00001511099344031543`
  - `%OCE_FORWARDING-3-CAUSE_OCE_COUNTER_EXCEED_STACK: OCE counter stack exceed -`

  Conditions: This symptom is not caused by any specific conditions.

  Workaround: There is no workaround.

- CSCub70336

  Symptom: Router crashes when the **clear ip bgp *** command is done in huge scale condition.

Conditions: This issue is observed only when huge scale with ten of thousands of peers and lot of vpnv4/v6 prefixes.

Workaround: Issuing the **clear ip bgp *** command is not a common operation. A crash occurs when the **clear ip bgp *** command is issued . Do not perform this workaround.

- CSCub70819

  Symptom: No mechanism is available to upgrade the existing throughput licenses, for example, from throughput_10g to throughput_20g.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: Install the corresponding throughput license to get the throughput value.

- CSCub71570

  Symptom: The dynamic route-map counter displays wrong results.

  Conditions: This issue occurs when the **show route-map dynamic** command is in the **more** state and a trigger clears the clear route-map entries.

  Workaround: Avoid executing the **show route-map dynamic** command in the **more** state for long and use terminal length 0 before displaying the **show** command output.

- CSCub73403

  Symptom: Bad voice quality.

  Conditions: some possible conditions that may update the trigger conditions later 1. RP1, ESP10, SIP10 2. This issue may be impacted by the multiple spa 0/0 SPA-2X1GE-V2 ok 17:46:43 0/1 SPA-DSP ok 16:18:57 0/2 SPA-2X1GE-V2 ok 17:46:42 3. Transcoding / blended transcoding.

  Workaround: There is no workaround.

- CSCub73484

  Symptom: The standby ESP100 gets reloaded.

  Conditions: 4K IKEv2 IPv6 static crypto map 4k VRF (ivrf = fvrf). Running bi-directional IMIX traffic @ 4Gbps for 5 minutes.

  Workaround: There is no workaround.

- CSCub73159

  Symptom: The IOSD crashes.

  Conditions: This issue occurs when you bring up 8k PPP sessions with QoS and EBGP routes.

  Workaround: There is no workaround.

- CSCub73177

  Symptom: The RP crashes.

  Conditions: This issue occurs when the Cisco router is reloaded.

  Workaround: There is no workaround.

- CSCub73430

  Symptom: Cisco router running on Cisco IOS 15.2.(4)S ipBaseK9 feature set will crash when an interface that a QoS policy attached to it is activated.

  Conditions: This issue occurs when a Cisco router is reloaded.

  Workaround: Use other feature sets, for example, AdvEnterpriseK9.

- CSCub76612

  Symptom: The console displays a message:

  ```
  %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image: PFR TT Enable download to CPP
  failed" and prints traceback
  ```

  The Cisco ASR1000 Series Aggregation Services Router may reload with the fman_fp core file.

  Conditions: FMAN-FP reports the PfR ERR log when a PfR session is flapping between MC and BR.

  Workaround: There is no workaround.

- CSCub77685

  Symptom: The CPU temperature reaches a high point with a water mark message.

  Conditions: This issue occurs in the SSO mode with L2VPN set up.

  Workaround: Use the standby in the RPR mode.

- CSCub78143

  Symptom: The **Clear ip bgp vpnv4 unicast damp rd** command does not clear the damp information in the VRF.

  Conditions: This issue occurs when you configure the BGP Dampening feature within the address family and flap the BGP route.

  Workaround: Use the **clear ip bgp vrf <***VRF name***> dampening** command.

- CSCub79590

  Symptom: The **match user-group** command does not appear in the running configuration after being configured. Configure an inspection type class-map.

  Conditions: This issue pertains only to the **match user-group** command.

  Workaround: This issue affects devices after reload because the corresponding router reads the startup configuration, which does not have the **match user-group** command. Therefore, the **match user-group** commands should to be re-entered after each reload.

- CSCub81374

  Symptom: The Cisco ASR1001 Feature Navigator does not show the correct image for license mapping.

  Conditions: ASR1001 ordering with or without licenses.

  Workaround: There is no workaround.

- CSCub82275

  Symptom: A Cisco ASR 1000 Series Aggregation Services Router may experience reloads on the ESP module due to a CPP driver fault during an in-2-out NAT translation. The issue has been notices in Cisco IOS 15.2S, but not in 15.1S.

  Conditions: The issue occurs when NAT is enabled. No other known requirements have been identified.

  Workaround: Disable NAT or downgrade to a 15.1 release.

- CSCub83960

  Symptom: After the second RP switchover, mcast traffic stop forwarding by PE.

  Conditions: mVPN topo, during mcast traffic sending, do an RP switchover on PE1.

Workaround: Using the **clear ip mroute *** command to enable the global MDT mroute rebuild can restore the mcast traffic before and after the second switchover.

- CSCub84204

  Symptom: The GTPv0 request is dropped and there is a failure to create a session.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: There is no workaround.

- CSCub85608

  Symptom: An ASRNAT address leak may occur. This displays a larger number of allocated addresses inthe **sh ip nat stat** command output, as also the translations that exist for the corresponding IP address.

  Conditions: This issue occurs when a dynamic routemap configuration is used and the NAT subdrop code ESP_CREATE_FAIL is increments, that is, ESP traffic must be present.

  Workaround: The leaked addresses can be reclaimed periodically by executing the **clear ip nat trans** command in the nonpeak hours to avoid user disruption.

- CSCub85948

  Symptom: A memory leak occurs due to CDP protocol.

  Conditions: This issue occurs under normal working conditions.

  Workaround: Remove the **no cdp advertise-v2** command from the configuration.

- CSCub86706

  Symptom: After multiple RP switchovers, the router crashes with the following message:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP HA SSO
  ```

  Conditions: This issue occurs under the following conditions:

  - mVPN with 500 vrf
  - Performed multiple switchover on PE1

  Workaround: There is no workaround.

- CSCub88742

  Symptom: NULL pointer access in a BGP C-Route function

  Conditions: This issue occurs when MPLS MLDP is toggled after two SSOs and when each SSO takes a long time to complete because of an HA bulk sync failure in the IP multicast.

  Workaround: There is no workaround.

- CSCub89150

  Symptom: PW with backup.

  Conditions: This issue occurs when you switch between the active and standby pseudowire.

  Workaround: Reload the corresponding routers.

- CSCub89157

  Symptom: Message are dropped.

  Conditions: This issue occurs when the message string exceeds 128 charecters.

  Workaround: Resend the message.

- CSCub89711

Symptom: The **ATM** keyword for the **show** command disappears.

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

Workaround: There is no workaround.

- CSCub91150

  Symptom: The Cisco SBC interface cannot be pinged from a Cisco ASR 1000 Series Aggregation Services Router.

  Conditions: 1. SBC interface is created with netmask /32. 2. SBC activated.

  Workaround: 1. Deactivate SBC. 2. Delete the SBC interface and re-create it again.

- CSCub91178

  Symptom: ALG FTP44 does not work and the data path fails to get established.

  Conditions: This occurs when the two networks are divided into twoVRFs, with both the client and server residing.

```
Topo:
Client  --- Gi 0/0/0 --- vasileft 1 --- vasiright 1 --- Gi 0/0/1  ----  Server
(inside)       (outside)         (outside)        (inside)
vrf_in                                 vrf_out
```

  For vrf_in, there is a dynamic NAT:

```
access-list 10 permit 10.0.0.0 0.255.255.255
ip nat pool in 202.120.0.2 202.120.0.10 prefix-length 24
ip nat inside source list 10 pool in vrf vrf_in overload
```

  For vrf_out there is a static NAT:

```
ip nat inside source static 192.168.0.2 202.119.0.2 vrf vrf_out
```

  The client runs the FTP in the active mode.

  Workaround: Use dynamic NAT instead of ALG FTP44.

- CSCub92997

  Symptom: Router crashes after a session flap.

  Conditions: This issue occurs when the ... Router has a BGP Route Server enabled and has a route-server client with graceful restart enabled. A client-generated session flap will cause a crash.

  Workaround: Disable graceful restart.

- CSCub93228

  Symptom: Incorrect TCAM search key. Traffic does not pass through even if the filter conditions are met.

  Conditions: This issue occurs when IPv4 and IPv6 co-exist in the interface configuration, and FW NAT is configured.

  Workaround: Instead of using a pre-NAT source address in the ACL, use a post-NAT source address.

  If the static NAT `ip nat inside source static 36.1.1.2 37.1.1.83` is used, in order to allow traffic from host 36.1.1.2 to pass through the firewall, the ACL should be.

```
ip access-list extended foo-list
permit ip host 36.1.1.2 any
```

Due to this list, the ACL should be configured as follows:

```
ip access-list extended foo-list
permit ip host 37.1.1.83
```

- CSCub96074

  Symptom: Software is forced to reload on the Cisco ASR 1000 Series Aggregation Services Routers or RP2.

  Conditions: ISG sessions cannot be authenticated or authorized whenever primary or secondary RADIUS servers are marked as unreachable. This creates a high load on the ISG.

  Workaround: There is no workaround.

- CSCub96323

  Symptom: When the **aaa session-id unique** command is in place, the parent session ID in the service accounting request does not match the session ID of the corresponding user session.

  Conditions: This issue occurs when the **aaa session-id unique** command is configured in the ISG.

  Workaround: Remove the **aaa session-id unique** command and work with the default setting.

- CSCub96576

  Symptom: Reload may occur.

  Conditions: A reload may occur on a Cisco ASR 1000 Series Aggregation Services Router with NAT when removing static RMAP mapping.

  Workaround: There is no workaround.

- CSCub96743

  Symptom: Packet loss is seen during SSO swithover in the Cisco ASR 1000 Series Aggregation Services Routers platform.

  Conditions: This happens in scaled configurations.

  Workaround: Cisco has fixed it partially for loopback interfaces.

- CSCub97641

  Symptom: When a NetFlow test is performed in the NAT CGN mode, you may see an abnormal NetFlow log. However, this is not seen in the default mode. Use the template ID 257 instead of 256.

  Conditions: This issue occurs when ... is configured as c**gn mode : ip nat log translations flow-export v9 udp destination 10.75.163.59 9995 ip nat settings mode cgn.**

  Workaround: There is no workaround.

- CSCub98634

  Symptom: NTP clients are unable to synchronize properly with the NTP server.

  Conditions: **Ntp access-group serve** or **Ntp access-group serve-only** configured on the NTP server running 15.2 IOSXE-based version.

  Workaround: Revert back to 15.1 version or use the **Ntp access-group peer** command.

- CSCub99205

  Symptom: The shaper becomes inactive when policy-map rem/add back on sub-intf.

  Conditions: This issue occurs each time on rem/add on sub-intf.

  Workaround: Changing the shaper value reactivates the shaper.

- CSCuc00289

  Symptom: The interface cache is deleted when the **parser config cache interface** command is configured.

  Conditions: This issue occurs after the **show tech-support** command is issued.

  Workaround: Execute the **show running-config** command to create the interface cache.

- CSCuc00465

  Symptom: configured permit-error, for 3GPP RLS7&8 req/resp, sessions are created, but for those unknown/unwanted IE, gtp counter doesn't work correctly.

  Conditions: This issue occurs due to permit errors.

  Workaround: There is no workaround.

- CSCuc02916

  Symptom: The IPv6 packet with hop-by-hop extension header is dropped when the packet is sent out to the L2TP virtual access interface.

  Condition: ASR is configured as L2TP LNS. At that time, the EssUnsupPktType drop counter is incremented.

  Workaround: There is no workaround.

- CSCuc02921

  Symptom: An ESP crash occurs.

  Conditions: This issue occurs when SYN cookie protection is being triggered, and the packet TCP data offset is wrong.

  Workaround: Do not configure SYN cookie protection.

- CSCuc04837

  Symptom: On the serial interface, the Cisco IOS counters for input packets, input errors, and aborts increase even after the interface is administratively shut down.

  Conditions: This issue does not occur in any specific condition.

  Workaround: Shut down and restart the interface.

- CSCuc05660

  Symptom: The TTL in the CNAME record is reset.

  Conditions: DNS CNAME record.

  Workaround: There is no workaround.

- CSCuc05671

  Symptom: The console reports

  ```
  [aom]: (ERR): Unable to find async context for AOM and traceback.
  ```

  Conditions: This symptom occurs when FMAN-FP reports the PfR ERR log when a PfR session is flapping between the MC and the BR.

  Workaround: There is no workaround.

- CSCuc07235

  Symptom: When using the **call-policy-set copy source x destination y** command the na-src-name-anonymous-table is not copied.

  Conditions: This issue occurs if you reuse a number that was removed previously.

Workaround: Copy the policy to a new set number.

- CSCuc07317

  Symptom: The output of the **Show controller pos pm** command does not show the correct SFP line type for all the POS SPAs.

  Conditions: The line type is shown as LONG MM for all the SFPs inthe output of the **show controller pos pm frp** command.

  Workaround: Execute the **show hw-module subslot x/y transceiver** command.

- CSCuc08098

  Symptom: The trap configuration for the AAA-SERVER MIB is missing.

  Conditions: This issue occurs when a Cisco ASR 903 device is loaded with MetroAggrServices license.

  Workaround: There is no workaround.

- CSCuc09520

  Symptoms: Some transit ICMPv6 traffic may not be forwarded by instead processed by the device itself, even if the destination IPv6 address is not one of the IPv6 addresses configured on the device.

  Conditions: An IPv6 packet carrying an ICMPv6 payload and a hop-by-hop extension header, and within the HbH a Router Alert option for MLD will not be forwarded, but processed by the device itself.

  Workaround: Apply an ACL blocking the IPv6 packets carrying a hop-by-hop extension header. Note that such an ACL will also block legitimate MLDv1 or MLDv2 traffic, which in turn will impact the neighbor discovery process (including DAD).

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as at the time of evaluation were 2.6/2.3:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:P/I:N/A:N/E:F/RL:W/RC:C

  No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuc10081

  Symptom: ISSU and ISSD fail.

  Conditions: They fail under all conditions.

  Workaround: There is no workaround.

- CSCuc11853

  Symptom: The T1 Controller stays DOWN after switchover.

  Conditions: This issue occurs when the SATOP is configured on T1.

  Workaround: Use the **shut** and **no shut** commands.

- CSCuc13805

  Symptom: The LSP Tunnel Head Control process is seen holding memory over a period of time with higher count/memory held each time outputs are collected.

  Conditions: Explicit IDs are only released when defined with an address. When the IDs are stored as a string, no function releases them.

Workaround: Use Path Protection using Path Option Lists with ID-explicit paths rather than named explicit paths.

- CSCuc14088

  Symptom: The default class is not exported with the class option template.

  Conditions: The class-default class is missing in the c3pl-class-table under the Flow Exporter.

  Workaround: There is no workaround.

- CSCuc15203

  Symptoms: The Router crashes when you configure ZBFW.

  Conditions: The following conditions:

  – The ISM-VPN module is turned on.

  – Asymmetric routing occurs.

  Workaround: There is no workaround.

- CSCuc15548

  Symptom: Subscriber session on LAC/LNS with **vpdn authen-before-forward** and auto-service in the radius-profile

  Conditions: **vpdn authen-before-forward** command and one auto-service in the users profile.

  Workaround: Configure and apply a policy map with the SESSION-START rule.

- CSCuc15695

  Symptom: The counters are not polling the correct statistics.

  Conditions: This symptom was first observed on an ATM interfere, but is not particular to the ATM because this issue was reproduced on a Gigabit Ethernet interface as well.

  Workaround: There is no workaround.

- CSCuc16125

  Symptom: Packet drops may occur and syslog errors may be displayed during ISSU.

  Conditions: This issue is observed during ISSU.

  Workaround: There is no workaround.

- CSCuc16623

  Symptom: After changing the grandparent shape rate via ANCP, traffic is not shaped to the new rate.

  Conditions: PPPoE model F Qos. Through ancp, change the grandparent shape rate.

  Workaround: There is no workaround.

- CSCuc19783

  Symptom: BGP neighbor sessions are not reset when the router ID is changed in the BGP VRF address family.

  Conditions: This issue occurs when the router ID is not configured within the BGP VRF address family.

  Workaround: Manually reset the BGP neighbors in the VRF address family by issuing the **clear ip bgp vrf <***vrf-name***>** command.

- CSCuc19862

  Symptom: Traceback and CPUHog is seen due to spurious memory access when flexible NetFlow is enabled on a 4G cellular interface.

Conditions: Enable flexible NetFlow on a 4G cellular interface with the traffic rate set to 1Mbps.

Workaround: There is no workaround.

- CSCuc20045

  Symptom: The maximum configurable port bundle host key (PBHK) source interfaces on an Cisco ASR 1000 Series Aggregation Services Router is random and could be as low as 1.

  The following is a sample error message that is displayed on a Cisco ASR 1000 Series Aggregation Services Router when adding 83rd source interface for PBHK:

  ```
  PortBundle: Unable to add source IP into list PortBundle: Command failed  PortBundle: allowed number of source IPs: 82
  ```

  Conditions: Configure multiple PBHK source interfaces on the Cisco ASR 1000 Series Aggregation Services Router.

  Workaround: There is no workaround.

- CSCuc21880

  Symptom: A memory leak is observed in aaa_util_get_cmdlist.

  Conditions: A memory leak is observed in the aaa_util_get_cmdlist on Cisco 3945 Integrated Services Router after a 10-hour traffic run for spoke-to-spoke FlexVPN.

  Workaround: There is no workaround.

- CSCuc22217

  Symptoms: The multicast re-created state may take one minute to register.

  Conditions: Shutdown interface on first hop router towards active source and let multicast state time out, then bring up interface. This may delay recreated state with one minute.

  Workaround: There is no workaround.

- CSCuc25214

  Symptom: router crashes after-an SNMP MIB expression is enabled.

  Conditions: This symptom is not caused by any specific condition.

  Workaround: There is no workaround.

- CSCuc26232

  Symptom: A reload indicating **stuck thread** may occur.

  Conditions: On a clear ip nat translations vrf <vrf-name>

  Workaround: use clear ip nat trans. * This issue exists only in Cisco IOS XE Release 3.7.1.

- CSCuc26434

  Symptom: RP information is not learned when auto RP is configured for a customer domain and the MA and RP candidates are on different PEs.

  Conditions: MA and RP candidate are on different PE.

  Workaround: There is no workaround.

- CSCuc29310

  Symptom: The TD probes in fast mode are gone when the link flaps.

  Conditions: This issue occurs when a link flap causes an SAF session flap.

  Workaround: Clear **pfr mas tr.**

- CSCuc31692

Symptom: A Cisco ASR 1000 Series Aggregation Services Router ucode crash occurs during scaled MLPPP configuration with sustained high data rates across most bundles.

Conditions: This issue occurs during a highly scaled MLPPP configuration with sustained high data rates across most bundles. This symptom has been seen only in the context of ESP40.

Workaround: There is no known workaround.

- CSCuc33328

  Symptom: Memory leaks are found in the statistics.

  Conditions: This issue occurs when a probe is executed and statistics are updated.

  Workaround: There is no workaround.

- CSCuc34315

  Symptom: The Cisco ASR 1000 Series Aggregation Services Routers crash with fman_fp during the unconfiguring process during a PBR scalability test.

  Conditions: After the PBR scalability test is performed with 1024 interfaces, a crash is observed.

  Workaround: There is no workaround.

- CSCuc34574

  Symptom: Pending-issue-update @ SSL CPP CERT on ASR 1000, 1002, ESP-1000 platform.

  Conditions: show platform software object-manager fp active pending-issue-update Update identifier: 128 Object identifier: 117 Description: SSL CPP CERT AOM show Number of retries: 0 Number of batch begin retries: 0

  Workaround: There is no workaround.

- CSCuc36464

  Symptom: Traffic check fail for user-defined classes with HQoS policy.

  Conditions: This issue occurs on sending traffic from ixia.

  Workaround: There is no workaround.

- CSCuc37597

  Symptom: A memory leak is seen at the responder nodes during reverse mediatrace.

  Conditions: A memory leak seen at the responder nodes on receiving a proxy request and while receiving responses for reverse mediatrace.

  Workaround: There is no workaround.

- CSCuc38440

  Symptom: The following message is displayed with the tracebacks:

  ```
  %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED
  ```

  Conditions: This issue occurs during configuration or unconfiguration of match the message ID under class.

  Workaround: There is no workaround.

- CSCuc39329

  Symptom: SNMP SMALL CHUNK leaks occur when the copy operation is performed using the **snmp set** command.

  Conditions: When performing the copy entry task, memory leaks are found. If this task fails, the leaks occur. 1. same entry in queue (snmp_config_copy_add fail to add new entry) 2. Enqueue into the copy queue fails 3.if ServerAddreesRev1 is set.

Workaround: Free all the pointer entries for all the above three scenarios.

- CSCuc40585

  Symptom: A ucode crash occurs when gtp aic inspect packets.

  Conditions: This issue occurs when GTP AIC is configured.

  Workaround: There is no workaround.

- CSCuc41531

  Symptom: A forwarding loop is observed in the context of some PfR-controlled traffic.

  Conditions: This symptom is observed with the following conditions:

  – Traffic classes are controlled via PBR.

  – The parent route is withdrawn on selected BR/exit.

  Workaround: This issue does not affect configured or statically defined applications; it affects only the learned applications. Therefore, the learned applications can be used as one of the workarounds. Another option is to issue **shut** and **no shut** on PfR master or clear the related TCs with the **clear pfr master traffic-class** command, which fixes the issue until the next occurrence.

- CSCuc43337

  Symptom: VRF name is not present in the **sh run** command output.

  Conditions: This issue occurs for vrf path-jitter probe.

  Workaround: There is no workaround.

- CSCuc44774

  Symptom: A high RTT spike is seen during the UDP jitter operation.

  Conditions: This issue occurs when another application runs for more than 500 ms, without giving the IP SLA a chance to run.

  Workaround: There is no workaround.

- CSCuc47357

  Symptom: An unexpected Cisco ASR 1000 Series Aggregation Services Router crash is observed on Release 15.2(2)S2 SW. The crash occurred at line 3799 in ppp_cp.c, which is in the cp_process_confreq()—function—from the core decode: #0 __be_cp_process_confreq (ppp=0x7f50114689e8, cp_spec=0xc87fa0ec4f7f0000, cp=0x7f501035a57c, neg=0x7f50059a6084) at ../VIEW_ROOT/cisco.comp/ppp/core/src/ppp_cp.c:3799

  Below is a snippet of cp_process_confreq(). The cp_get_option_spec() returned NULL and ppp_debug_prot_s() de referenced it:

  ```
  option_spec = cp_get_option_spec(cp_spec, option_type);       ppp_debug_prot_s(ppp,
  PPP_DEB_OPTION_STALL,                                <<< Line 3799
  cp_spec->cp_protocol, option_spec->name);         return; ...  The function
  cp_get_option_spec() is expected to return NULL and later debug print was trying to
  dereference the NULL pointer .
  ```

  Conditions: This symptom was observed when more than 40 x Cisco ASR 1000 Series Aggregation Services Routers were upgraded to Cisco IOS XE Relesae 15.2(2)S2.

  Workaround: A protective fix has been added before the debug print.

- CSCuc50498

  Symptom: A cpp_cp_svr crash is observed.

  Conditions: This issue occurs when the service policy is attached to a member link that has a port channel configured.

Workaround: There is no workaround.

- CSCuc57965

  Symptom: The ISG prepaid idle timer stops firing after receiving two QV0 in a roll from the prepaid sever.

  Conditions: This issue occurs when the ISG session with prepaid service is applied. After receiving two QV0 in a roll from the prepaid server, the prepaid idle timer stops firing, resulting in ISG stops contacting the prepaid server for more quota.

  Workaround: There is no workaround.

- CSCuc58513

  Symptom: FP reload occurs.

  Conditions: ALG traffic with ACL limit configuration.

  Workaround: Remove ACL limit configuration with ALG traffic.

- CSCuc58603

  Symptom: When using SNMP to query the CLNS adjacency table in the CISCO-IETF-ISIS-MIB, the ciiISAdjIPAddrType for IPv6 addresses is incorrectly reported as IPv4(1).

  Conditions: ISIS adjacency with IPv6 enabled.

  Workaround: There is no workaround.

- CSCuc60435

  Symptom: Packets with a single-digit MNC are not matched in the L7 class map. Instead, counters increase in the class, as follows:

```
Service-policy inspect gtpv1 : gtpv1_grx_inside_mcc_mnc
Class-map: gtpv1_grx_inside_mcc_mnc (match-any)
    0 packets, 0 bytes                  <<<< zero
    30 second offered rate 0000 bps
    Match:  mcc xxx mnc 1
    Match:  mcc xxx mnc 1
Class-map: class-default (match-any)
    543464 packets, 11565497 bytes  <<<<
    30 second offered rate 19000 bps, drop rate 0000 bps
    Match: any
```

  Conditions: This symptom is observed when the match criteria in the L7 class map define single-digit MNC as follows:

```
class-map type inspect gtpv1 match-any gtpv1_grx_inside_mcc_mnc
    match mcc xxx mnc 1
    match mcc xxx mnc 1
```

  Workaround: There is no workaround.

- CSCuc65437

  Symptom: A cpp_cp_svr crash is seen.

  Conditions: This issue occurs when service policy is removed from main int.

  Workaround: There is no workaround.

- CSCuc65609

  Symptom: Duringa SIP attack, NAT causes ESP lock-up.

  Conditions: This issue occurs because of a SIP registration attack.

Workaround: Use ACL to block the SIP attack.

- CSCuc67468

  Symptom: The **sh plat h q a f nat data dynbin** command output gets into a loop.

  Conditions: This issue occurs when the command is executed on a Cisco ASR 1000 Series Aggregation Services Router.

  Workaround: Use the **sh ip nat trans** command and its filters for showing this information.

- CSCuc67687

  Symptom: The Router crashes due to VRF-related RG configurations.

  Conditions: This condition is observed in the following configuration:

```
R1-13RU(config-if)# ip vrf forwarding b2b-vrf  % Interface GigabitEthernet0/1/0
R1-13RU(config-if)# ip address <ip> <mask>
R1-13RU(config-if)# zone-member security Z1
R1-13RU(config-if)# redundancy group 1 ip <ip> exc dec 50
```

  Workaround: There is no workaround.

- CSCuc74548

  Symptom: Due to overload, the console is locked.

  Conditions: Overload related problem.

  Workaround: There is no workaround.

- CSCuc76670

  Symptom: The 2X1GE-SYNCE (metronome) SPA does not boot on a Cisco ASR 1002 Router.

  Conditions: From release 3.7, the metronome SPA (2X1GE-SYNCE) fails to boot on a Cisco ASR 1002 Router. The following error message is displayed on the RP console:

```
SPA not supported.
```

  Workaround: There is no workaround.

- CSCuc78320

  Symptom: QFP crash with icmpv4 error packets when ZBF debugs enabled (**debug platform hardware qfp active feature firewall datapath global all detail**)

  Conditions: This issue occurs when the ZBF debugs are enabled.

  Workaround: Do not enable the ZBF debugs with the **detail** or **drop** keywords for all traffic. Enable ZBF debugs only for the traffic you would like to debug. See CSCtf45361 for more information.

- CSCuc88112

  Symptom: Ucode crashes.

  Conditions: This condition is observed while the frf12 feature is tested.

  Workaround: There is no workaround.

- CSCud27293

  Symptom: Sometimes, on a Cisco ASR1000 Series Aggregation Services Router, the SPA-8XT3/E3 SPA may not come up and may get powered off with the following message:

```
%SPA_OIR-6-OFFLINECARD: SPA (SPA-8XT3/E3) offline in subslot
```

  Conditions: This symptom occurs only on a certain set of on board flash devices on the SPA-8XT3/E3 with 15.3(01)S release.

  Workaround: There is no workaround.