Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7S

This chapter provides information about the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7S.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.7S

This chapter contains the following section:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.7S

This section documents resolved issues on Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.7S.

Identifier	Description
CSCuq59131	IOS XE L4 Redirect Crafted Packet Denial of Service Vulnerability
CSCub68073	IOS XE Crafted IPv6 Packet Denial of Service Vulnerability
CSCur02734	IOS-XE evaluation for CVE-2014-6271 and CVE-2014-7169
CSCus69732	IOS-XE: Evaluation of glibc GHOST vulnerability - CVE-2015-0235

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.6S

This chapter contains the following section:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.6S

This section documents resolved issues on Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.6S.

- CSCud94511

  Symptom: Multiple Tracebacks seen.

  Conditions: Router reload. The tracebacks are seen if a scaled configuration is present on any atm/gig spa with POS spa present in the system. Triggers can also vary from router reload to sip reload or shut/no shut of large number of tunnels. Triggers increase the load on router processing the interferes with the working of POS spa and hence tracebacks are seen.

  Workaround: There is no workaround.

- CSCuh97943

  Symptom: The following messages are output on ASR1001 running fixed version of CSCud57841.

  ```
  *Jul 8 08:17:08.264:%SMC-2-BAD_ID_HW: SIP0/1: Failed Identification Test in 0/1/4 [2/0] *Jul 8 08:17:08.840:%SMC-2-BAD_ID_HW: SIP0/0: Failed Identification Test in 0/0/3 [5/0]
  ```

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCui59300

  Symptom: ASR1002X LED's color mismatch to CLI status for built-in ports Gi0/0/0.

  Conditions: step1: write erase step2: reload.

  Workaround: Confirm the LED color.

  ```
  [A1KX-1]gig0/0/0   [A1KX-2]gig0/0/0 stage 0           shut: OFF               shut: OFF stage 1          no shut: Amber        shut: Green   <--[A1KX-2] is shut, but the LED is “Green”. stage 2          no shut: Green      no shut: Amber <--[A1KX-2] is no shut, but the LED is “Amber” Workaround: no shew--> shew again stage 3          no shut: Amber       shut: OFF shew--> no shew again stage 4         no shut: Green no shut: Green.
  ```

- CSCuj23603

  Symptom: The ESP may crash in cpp_mcplo %CPPHA-3-FAULT: F0: cpp_ha: CPP:0.0 desc:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR(interrupt) class:OTHER sev:FATAL id:2121 cppstate:RUNNING res:UNKNOWN flags:0x7 cdmflags:0x8.

  Conditions: NAT is enabled and mode has been changed between "Classic"/default and CGN.

  Workaround: Reload box or at least CPP after changing the mode.

- CSCuj57479

Symptom: Static Pat entries do not work and do not show up in the show ip nat translations output.

Conditions: When using both TCP and UDP port on the physical interface in the static pat configuration.

Workaround: Instead of specifying interface x overload, use the ip address of the interface.

```
Example: ip nat inside source static tcp 10.1.1.1 6666 interface gig 0/1 56666  use
this  ip nat inside source static udp 10.1.1.1 6666 192.168.1.1 56666     (
192.168.1.1 is the interface ip itself)
```

- CSCum04472

  Symptom: After performing a scaled configuration, removing an existing channel and adding a new one leads to trace back.

  Conditions: On b-b Patriot/Prowler setup, configure more than maximum allowed ds0 channels. Once the maximum no of channels are created, delete couple of them and recreate new ones.

  Workaround: There is no workaround.

- CSCum19739

  Symptom: fp crash with ip nat cgn mode enable.

  Conditions: 1. Configure NAT pool overload, start 300cps sip traffic including NAT and non-NAT, 2. enable cgn mode with "ip nat setting mode cgn"

  Workaround: There is no workaround.

- CSCum37911

  Symptom: With TBAR enabled, dataplane traffic may be dropped in a GetVPN environment with mixed GMs (ASR and ISR) when there is a change in the NTP clock.

  Conditions: GetVPN configuration with TBAR, and NTP clock is changed.

  Workaround: 1) Adjust the NTP server to the current clock or, 2) Re-register the ASR GM with the KS using 'clear crypto gdoi' or, 3) Disable TBAR.

- CSCum54014

  Symptom: ESP reloads after reporting one or both of the following interrupts:
  CGI_CSR32_CGI_OTHER_LEAF_INT__INT_YIC_M40_TIMEOUT
  PIT_CSR32_PIT_HPI_MISC_LEAF_INT__INT_HPI_ISN_INVALID_ADDRESS_INT

  A ucode core file may or may not be created when this event occurs.

  Conditions: Only applies to ESP100, ESP200 and ASR1002-X.

  Workaround: The issue is fixed in releases: 15.2(4)S6 / XE3.7.6S 15.3(3)S4 / XE3.10.4S 15.4(1)S3 / XE3.11.3S 15.4(2)S / XE3.12.0S 15.4(3)S / XE3.13.0S.

- CSCum55564

  Symptom: Memory leak is observed.

  Conditions: If ISG receives CoA request for a session that does not exist, logged memory leak is observed.

  Workaround: Send CoA request only for existing session.

- CSCum56514

  Symptom: A Cisco router running IOS XE may crash and reload after generating a ucode core file and logs similar to the following:

  ```
  Notice 1531: KRZ: SIP0: pvp.sh: Process manager is exiting: process exit with reload
  fru code Error 1530: KRZ: SIP0: cpp_cp: cpp_cp encountered an error -Traceback=  Error
  1529: KRZ: SIP0: pman.sh: The process cpp_ha_top_level_server has been helddown (rc
  ```

```
69)   Error 1528: KRZ: SIP0: pman.sh: The process cpp_cdm_svr has been helddown (rc
69)   Informational 1526: KRZ: F0: cpp_ha: Shutting down CPP MDM while client(s) still
connected   Informational 1525: KRZ: SIP0: cpp_cdm: Shutting down CPP MDM while
client(s) still connected  Informational 1527: KRZ: F0: cpp_ha: Shutting down CPP CDM
while client(s) still connected  Error 1524: KRZ: F0: cpp_ha: CPP 0 microcode
crashdump creation completed.
```

Conditions: A Cisco router running IOS XE and traffic passing through the NAT path.

Workaround: There is no workaround.

- CSCum78930

  Symptom: The ICMPv6 error packet (too-big packet) with icmpv6 echo reply as payload is dropped by ZBFW.

  Conditions: If the intermediate hosts generate icmpv6 error packets with icmpv6 echo reply as pay load without properly fragmenting the packets as per the mtu of the v6 packet flow, such icmpv6 errors packets are dropped.

  Workaround: Adjust the mtu of the v6 pack flow so that packets, especially the icmvp6 echo reply does not generate an error (too-big message).

- CSCum90509

  Symptom: No RTP Connections for RSVP Features in Cisco IOS Release XE 3.7 image.

  Conditions: This symptom is observed Only for RSVP call.

  Workaround: Use the version where CSCuj58299 is not integrated.

- CSCum99077

  Symptom: fman_rp process crashes. RP card reloads.

  Conditions: When routing loop occurs in a network and causes massive routing information update, an internal logic error may be triggered.

  Workaround: Avoid routing loop.

- CSCun09640

  Symptom: The following errors are seen when adding a child policy to a parent policy while configuring hierarchical QoS.

  ```
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp:  cpp_cp encountered an error   %CPPOSLIB-3-
  ERROR_NOTIFY: F0: fman_fp_image:  fman-fp encountered an error  %PMAN-3-PROCHOLDDOWN:
  F0: pman.sh:  The process cpp_ha_top_level_server has been helddown (rc 69)  %PMAN-3-
  PROCHOLDDOWN: F0: pman.sh:  The process cpp_cp_svr has been helddown (rc 134)    This
  can result in a ESP (F Fabric) reload, causing a traffic outage    *Feb 13
  07:39:05.829: %IOSXE_OIR-6-ONLINECARD: Card (fp) online in slot F0
  ```

  Conditions: 1. An interface with a service-policy applied. 2. Replacing the child policy on the parent hierarchical policy applied to the interface.

  Workaround: Remove the policy from the interface before making the changes to the child/parent policy then reapply the policy to the parent. OR If you issue the no command to remove the child policy from the parent and then query for pending configuration objects using the s**how platform software object-manager fp active statistics** command to make sure there are no pending objects, then issue the service-policy to add the new child policy to the parent, you will not see the ESP crash.

- CSCun09973

  Symptom: A vulnerability in the Layer 2 Tunneling Protocol (L2TP) module of Cisco IOS XE on Cisco ASR 1000 Series Routers could allow an authenticated, remote attacker to cause a reload of the processing ESP card. The vulnerability occurs during the processing of a malformed L2TP

packet. An attacker could exploit this vulnerability by sending malformed L2TP packets over an established L2TP session. An exploit could allow the attacker to cause a reload of the affected ESP card.

Conditions: Device is configured with the **no vpdn ip udp ignore checksum** command.

Workaround: There is no workaround.

- CSCun13999

  Symptom: Under interface superscription condition we might see the following error message on router console: %CMCC-3-PLIM_STATUS: SIP0: cmcc: A PLIM driver informational error TXMC0 - txmcBufferOverflow, block 1f count c8.

  Conditions: When "fair-queue" is used in QoS policy-map, under interface subscription condition the flow-control between BQS and SPA might excommunicate, hence the error message is printed.

  Workaround: There is no workaround.

- CSCun17558

  Symptom: COS markings not seen proper on the dot1q interface.

  Conditions: The issue is seen if met all of following conditions: 1, MPLS packets with fragment happened in data plane on the dot1q interface.

  Workaround: There is no workaround.

- CSCun20274

  Symptom: Standby RP source is not participating in clocking selection.

  Conditions: We must have the below specific netclk config on the ASR1k and need to perform RP-switchover. "network-clock select 1 BITS R0 <T1/E1> <Framing>" "network-clock select 2 BITS R1 <T1/E1> <Framing>".

  Workaround: Remove and re-apply the stby-network-clk Source with different framing.

- CSCun20279

  Symptom: At uRPF loose mode, the suppress drop counter on ASR1K will count packets even in case the packets are symmetric flow. ASR1K should not count symmetric flow packets as sdrop at uRPF loose mode.

  Conditions: uRPF loose mode.

  Workaround: There is no workaround.

- CSCun24965

  Symptom: On a ASR1000 series router, configuring a QoS service policy using the service-fragment type, the shaping value is not correct.

  Conditions: A QoS Service Policy is applied using the service-fragment keyword, the shaped value is not correct.

  Workaround: There is no workaround.

- CSCun28171

  Symptom: An ISG stops processing CoAs for a subscriber session when CoAs are received in rapid succession. The received CoAs are queued but never processed.

  Conditions: This symptom occurs when multiple CoAs for a single subscriber session are received in short time (milliseconds).

  Workaround: The subscriber session needs to be reset to recover.

- CSCun28965

Symptom: "**show ip nat translation filter range [inside | outside] [local|glocal] <start-ip> <end-ip>**" command does not filter the output as per the range specified.

Conditions: This symptom occurs on Cisco ASR 1000 Series router.

Workaround: There is no workaround.

- CSCun38287

  Symptom: ISG users can not online with 3 services on 3.7.4 with "vpdn authen-before-forward". But can online with 3.7.2.

  Conditions: 3.7.4 image and "vpdn authen-before-forward" configured.

  Workaround: remove "vpdn authen-before-forward". or downgrade to 3.7.2.

- CSCun48994

  Symptom: The CP process crashes while collapsing a hierarchy layer node that had once exceeded 4000 entries. The collapse occurs when the number entries falls below 4000.

  Conditions: This problem occurs while collapsing a node that had once exceeded 400 entries. The problem is specific to MLPPP, MFR and GEC aggregate because these features require notification when a schedule ID changes. The schedule ID changes when a scheduling node is reconstructed. The issue hit when the operation involves both the flushing and SID notification.

  Workaround: There is no workaround.

- CSCun69811

  Symptom: Customer on active box would only like to "no activate" a single delegate registration entry below.

  ```
  subscriber sip: 999999@site.com      sip-contact sip: 001999999999@10.0.0.1
  adjacency CUCM-llab      delegate-registration sip:test.site.com        adjacency
  PSTN-lab-SIP-CONNECT-test-lab       profile SIP-CONNECT_TIMERS       activate
  ```

  Conditions: Sessions are deactivated and the stand-by router crashes.

  Workaround: "no activate" command must be executed at the "delegate-registration" sub section. This will prevent the deactivation of the sessions.

- CSCun75848

  Symptom: When High Rate of CoA are sent for a very long period of time, the process ISG CMD HANDLER might hog the CPU at a very high value.

  Conditions: CoA sent for a very long time at a very high rate (Several hours).

  Workaround: There is no workaround.

- CSCun78318

  Symptom: ACLs applied to the mgmte do not work on the new active RP after a RP switch over.

  Conditions: After a RP switch over as the old standby RP becomes the new active RP.

  Workaround: Remove and reapply the ACLs to the mgmte on the new active RP.

- CSCun87685

  Symptom: ASR1006/15.4(1)S crashed while adding port and host specific deny statements on specific lines for the WCCP-Redirect ACL.

  Conditions: Adding port and host specific deny statements on specific lines for the WCCP-Redirect ACL.

  Workaround: There is no workaround.

- CSCun89036

Symptom: Traceback when IPV6 traffic is transiting through ATM sub-interface.

Conditions: Configuration of "atm route-bridged ipv6" configured at ATM sub-interface level.

Workaround: There is no workaround.

- CSCun91199

  Symptom: NAT ALG not translating in case of multiple sip address in SDP.

  Conditions: sip invite message containing oline and cline with different addresses and both need translation dynamic nat with acl configured.

  Workaround: Simplify the ACL associated with NAT mapping configuration.

- CSCun96598

  Symptom: SNMP query on DS3-MIB objects like dsx3LineLength, dsx3LineStatusLastChange, dsx3LoopbackStatus and dsx3Channelization are showing value 'zero' for SPA-2XT3/E3 card.

  Conditions: Test DS3-MIB objects on 2XT3/E3.

  Workaround: There is no workaround.

- CSCun96969

  Symptom: The ASR1002 running IOS_XE 3.7.0 (15.2(4)S) crashed after a configuration change inf

  ```
  FNF.  %FMANRP_NETFLOW-3-INVALIDFLOWDEFCPP: CPP Flow definition can not be  created 1
  Mar 19 12:18:33 lns3 1596693: -Traceback=  1#fcbfdf6899eea283341cebf8c5320ad1
  :10000000 6FBFE8 :10000000 6FC394  :10000000 5B9F54C fnf_config:9DB4000 1B270
  fman_rp:ED4B000 1D0 764 fman_rp:ED4B000 1D0954 :10000000 3326E78 :10000000 330110C Mar
  19 12:18:33 lns3 1596694: Mar 19 12:18:32.268:
  ```

  Conditions: An FNF record that includes one of the following key/non-key fields configured along with an extracted field will trigger the trace back, one or more fields derived from the below: match/ collect routing source/destination [peer] as [4-octet] along with an extracted field such as: collect application http host Example: flow record test-rec match routing source as 4-octet collect application http host flow monitor test-mon record test-rec.

  Workaround: There is no workaround.

- CSCun97760

  Symptom: ASR running 15.2(4)S4 saw ESP crash due to corrupted H323 packet.

  Conditions: ASR running 15.2(4)S4 saw ESP crash due to corrupted H323 packet.

  Workaround: If customer does not need h.323 alg, a workaround is to disable h.323 alg: no ip nat service h225.

- CSCuo09390

  Symptom: ASR1K crash on netflow configuration change.

  Conditions: When all current CVLA client features are unconfigured and registration happens from beginning for a new client, allocating initial chunk memory fails. The following are the ASR1k features capable of using CVLA currently, FNF NBAR CFT OneFW MCP Connected Enterprise (CENT) CPP Flow Metadata (FMD) CPP Flow Metric Engine (FME) AppNav vPath Flow Object/ Service Controller.

  Workaround: Do not unconfigure every existing CVLA feature at once. Leave atleast one feature configured so that when a new feature is configured, CVLA does not have to allocate the initial chunk memory again. Leaving out atleast one CVLA feature configured will avoid the crash. Note: The following are the ASR1k features capable of using CVLA currently, FNF NBAR CFT OneFW

MCP Connected Enterprise (CENT) CPP Flow Metadata (FMD) CPP Flow Metric Engine (FME) AppNav vPath Flow Object/Service Controller. To view the list of features currently configured on your box to use CVLA, use the show command **sh plat hard qf a infra cvla client handles .**

- CSCuo15649

  Symptom: On 10 Gig Ports, with traffic of packet size 9216 bytes, a traffic drop is noticed The code changes made for the application of new initialization sequence for the serdes device is causing the issue, hence reverting the changes.

  Conditions: Hence Backing out the DDTS.

  Workaround: There is no workaround.

- CSCuo20090

  Symptom: The saved ACLs applied to the mgmte from startup-config may not work after system reload.

  Conditions: After system reload.

  Workaround: Remove and reapply the ACLs to the mgmte after system reload.

- CSCuo29770

  Symptom: ESP fails to initialize and reboots. A message like the following will be seen on the IOS console:

  ```
  *Jan 01 16:22:35.562: %CPPHA-3-INITFAIL: F0: cpp_ha:  CPP 0 initialization failed - startup init (0x1)    *Jan 01 16:22:35.562: %CPPHA-3-INITFAIL: F0: cpp_ha:  CPP 0 initialization failed - start CPP (0x1)
  ```

  The cpp_driver tracelog contains an entry which lists an A41C error code, indicating that the driver was unable to turn on termination. Here is an example:

  ```
  01/01 16:22:35.120 [cpp-drv]: (ERR): COMP0053/dui/A41C: QFP0.0 - unable to turn on termination for DUI0
  ```

  This is an intermittent failure, so the ESP will likely initialize successfully on the 2nd or 3rd attempt. This is an initialization issue, and once initialization completes successfully there are no further problems related to this condition.

  Conditions: Only ASR1002-x, ESP100 and ESP200 are affected. Router configuration or traffic pattern do not affect this problem. The software is fixed in XE3.7.6S, XE3.10.4S, XE3.11.2S, XE3.12.0S and later releases.

  Workaround: There is no workaround.

- CSCuo38164

  Symptom: Traceback and log error noticed.

  Conditions: While initiating H323 call with SBC feature.

  Workaround: There is no workaround.

- CSCuo52384

  Symptom: ROMMON get_mac_addr and IOSXE IDPROM access fail on booting standby RP2.

  Conditions: External USB thumb drive used on RP2.

  Workaround: Remove external USB thumb drive on RP2.

- CSCuo55610

  Symptom: Incomplete kernel core file with filename ending in TEMP_IN_PROGRESS.

  Conditions: Active RP kernel core dump in dual RP2 systems.

  Workaround: There is no workaround.

- CSCuo61982

  Symptom: At uRPF loose mode, the suppress drop counter on ASR1K will count packets even in case the packets are in symmetric flow. ASR1K should not count symmetric flow packets as sdrop at uRPF loose mode.

  Conditions: uRPF loose mode.

  Workaround: There is no workaround.

- CSCup30822

  Symptom: The Tensilica license server is moved from Solaris to Linux boxes (move 7030@ls-na-west to 51213@ls-sjc-01, and move 7030@ls-na-east to 51213@ls-rtp-01). Any files which contain 7030@la-na-* need to be changed to new Linux server and port.

  Conditions: The licenses have been rehosted to another server/port, but there are changes needed in any branch that is still active as of the decommission date that needs to build any image based on the CPP10/Yoda ucode images (any of the asr1k and ubr based images but excluding the csr/ultra and isr/utah/sword/dagger/overlord/juno). The Solaris machines will be decommissioned on July 18, 2014. After this time, CPP10/Yoda ucode images without these changes will fail to build. If you have a private development branch that you expect to be active after the decommission date you will want to double commit CSCup30822 to your branch as well (or sync to pickup those changes). Note that xe37_throttle requires CSCtz95343 as well as the xe37 diffs.

  Workaround: There is no workaround.

- CSCup39448

  Symptom: The show interface counter doesn't increase on partial Serial line with ASR1001-8XCHT1E1.

  Conditions: The stats update is skipped rest of the VC's in that port if one interface is down in that port. All of channelized T1/E1 modules running IOS-XE 3.7.2S (or after) potentially exists this problem. If the first I/F is UP, all of the I/Fs don't count up. 2) Even if the first I/F is UP, one I/F of which next I/F has become down doesn't count up.

  Workaround: Explicitly shutdown the interface which is in down state.

- CSCuq09004

  Symptom: After upgrading the ASR to the latest 15.2(04)S and later 15.X releases the ASR1K started crashing. The trigger for this crash is when a flat QoS policy with fair-queue is applied to a frame-relay interface.

  Conditions: The trigger for this crash is the flat QoS policy with fair-queue applied to the frame-relay interface. In this case the two key components that together triggered this failure was the frame-relay plus the flat policy with fair-queue.

  Workaround: The workaround is to convert this flat policy to a hierarchical policy with a parent shaper set to 100%. policy-map PM_POS_PARENT class class-default shape average percent 100 service-policy PM_POS ! interface POS0/1/0 no ip address encapsulation frame-relay load-interval 30 crc 32 pos scramble-atm frame-relay lmi-type ansi service-policy output PM_POS_PARENT <? New hierarchical policy hold-queue 4096 out.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.5S

This chapter contains the following sections:

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.5S

This section documents the unexpected behavior that might be seen in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.5S.

- CSCte77398

  Symptom: A Cisco ATM router configured with ATM PVC Range commands report the following error when attempting to configure a PVC Range: `Unable to configure PVC Range. Possibly multiple users configuring IOS simultaneously`.

  Conditions: This problem occurs randomly and even if there are no multiple sessions accessing the pvc-range at the same time.

  Workaround: There is no workaround.

- CSCtw52699

  Symptom: Error seen on debug when disconnecting the session.

  Conditions: When a single session of ppoe is brought down this issue is seen.

  Workaround: There is no workaround.

- CSCtx72973

  Symptom: Config-sync failiure is seen when unconfiguring the crypto gdoi group.

  Conditions: Seen on HA setup.

  Workaround: There is no workaround.

- CSCty79442

  Symptom: On ATM BRAS it is not possible to configure vdpn-template under pvc-in-range configuration.

  Conditions: Basic configuration

  Workaround: There is no workaround.

- CSCtz49200

  Symptom: OSPF IPv6 control packets are not encrypted/decrypted.

  Conditions: This symptom is observed while configuring the IPv6 OSPF authentication.

  Workaround: There is no workaround.

- CSCtz75816

  Symptom: NBAR Field Extraction (AKA collect through IPFIX) does not work for flows over IPv6 tunnels.

  Conditions: 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.

- CSCua21238

Symptom: Cisco IOSd crashes at ipv6_address_set_tentative.

Conditions: This symptom occurs while unconfiguring IPv6 subinterfaces during the loading phase of a box with Netflow configuration.

Workaround: There is no workaround.

Symptom: iosd crashes @_ipv6_address_set_tentative

Conditions: While unconfiguring ipv6 subunterfaces

Workaround: There is no workaround.

- CSCua67748

  Symptom: If there are several monitors using same exporter, the exporter stats show exported stats in a cumulative way for all monitors. For example, 1st monitor 10, second monitor 20 while each of the monitors had just ten entries.

  Conditions: If same exporter is used with several monitors.

  Workaround: There is no workaround.

- CSCua90097

  Symptom: FlexVPN client ikev2 sa stuck at IN-NEG with status description: `Initiator waiting for AUTH response`

  Conditions: FlexVPN server initiate clear crypto session command to clear 4K crypto sessions. After crypto session recovered, there is 1 ikev2 sa at flexVPN client stuck at IN-NEG status. At flexVPN server, there is no ikev2 peer.

  Workaround: FlexVPN client is able to use clear crypto ikev2 sa psh index command to delete stuck ikev2 sa.

- CSCub00482

  Symptom: 2 IKEv2 sa created on a crypto session at flexVPN Server.

  Conditions: system bootup with 4K activity flexVPN clients and data traffic

  Workaround: There is no workaround.

- CSCub23971

  Symptom: An Access-Request sent by a BRAS might miss ANCP-attributes.

  Conditions: This symptom is observed if an ANCP-enabled subinterface is set up the first time or it gets removed/readded.

  Workaround: Reconfigure the ANCP neighbor name.

  Symptom: An Access-Request send by a BRAS might miss ANCP-attributes.

  Conditions: This is seen, if an ANCP-enabled subinterface is set up the 1st time or it gets removed/re-added.

  Workaround: Re-configure the ANCP neighbor name.

- CSCub54188

  Symptom: RP Crash.

  Conditions: TC services with timer expirying.

  Workaround: There is no workaround.

- CSCuc23498

  Symptom: fail to make blended transcode

Conditions: None.

Workaround: There is no workaround.

- CSCud11564

  Symptom: After Unconfigure/reconfigure a ATM pvc-bundle subinterface, it shows the new pvc pdindex is created and used but the orginal pvc dpindex not removed.

  Conditions: configure atm pvc-bundle under atm sub-interface

  Workaround: There is no workaround.

- CSCud31165

  Symptom: Shimdb entries does not clear even after all sessions get disconnected.

  Conditions: This symptom is observed when 2 different policy maps have same hash key when added to the shim_db tree. Issue happens because collision was not handled in the code.

  Workaround: There is no workaround.

- CSCud41480

  Symptom: QFP may reload.

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

  Workaround: There is no workaround.

- CSCud68778

  Symptom: Reset reason is not correctly displayed for some of the IOS-XE reloads.

  Conditions: Issue is seem when IOS-XE reloads due to punt path keepalive failure.

  Workaround: There is no workaround.

- CSCud71878

  Symptom: If an IPv6 PPPoE session is rapidly deleted/recreated multiple times then the following error message may be reported: %INTERFACE_API-3-NODESTROYSUBBLOCK: The SWIDB subblock named IPv6 Routing was not removed

  Conditions: None.

  Workaround: There is no workaround.

- CSCud86991

  Symptom: On ASR1K, the IOSd process may crash with "crypto dynamic-map" config.

  Conditions: When "crypto dynamic-map ..." is entered from CLI.

  Workaround: There is no workaround.

- CSCud90647

  Symptom: Abnormal output after ?show debug? on MCP_DEV_LATEST_20121219_080028 . No problem on mcp_dev 20121210

  Conditions: show debug

  Workaround: no

- CSCue29595

  Symptom: SRTP passthrough for h323 calls failing

  Conditions: h323 calls are failing when both the legs are h323 and its SRTP passthrough

Workaround: There is no workaround.

- CSCue66087

  Symptom: No translations are shown in "sh ip nat tr"

  Conditions: Send non pattable traffic and then send pattable traffic with same ip

  Workaround: There is no workaround.

- CSCue92716

  Symptom: Variable Length exceeds 256 chars might cause issues.

  Conditions: traffic with HTTP extracted fields with length exceeded 1 byte.

  Workaround: use traffic with http fields length less than 1 byte

- CSCug05130

  Symptom: IOSd core happened on NAT performance test.

  Conditions: nat rtsp traffic or nat ftp traffic.

  Workaround: There is no workaround.

- CSCug27362

  Symptom: Packet drop occurs when IPSEC VTI IPv6 tunnels are configured on an ESP80. Also getting the following message when the problem happens: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.1 Thread:207 TS:00000001059562400712 %ATTN-3-SYNC_TIMEOUT: msecs since last timeout 1035639, missing packets 6040

  Conditions: Packet drop occurs when IPSEC VTI IPv6 tunnels are configured on an ESP80. Also getting the following message when the problem happens: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.1 Thread:207 TS:00000001059562400712 %ATTN-3-SYNC_TIMEOUT: msecs since last timeout 1035639, missing packets 6040

  Workaround: The only workaround so far is to remove the IPSEC configuration between the tunnels.

- CSCug47592

  Symptom: PLIM Driver Error Messages observe while booting

  Conditions: On ASR1002-X router during booting

  Workaround: There is no workaround.

- CSCug60382

  Symptom: NTE payload type is renegotiated as asymmetric which some device cannot support

  Conditions: Mid call late invite to trigger renegotiated and the answer in SDP from initiator has different nte payload type as nte payload from offer 200(invite) in other side.

  Workaround: Remove nte payload in ACK using lua script

- CSCuh09580

  Symptom: With IOS-XE 3.7.3S on ASR1K and global crypto ikev2 dpd configuration, all crypto sessions have dpd enabled as expected, after performing RP Switch-Over, the crypto ikev2 dpd configuration is missed, all crypto session are re-established with dpd disabled.

  Conditions: DPD and RP Switch Over

  Workaround: There is no workaround.

- CSCuh20209

  Symptom: ucode crash on clear ip nat translations

Conditions: Very rarely with stateful traffic

Workaround: Use clear ip nat translations vrf <vrf_name> to clear vrf aware translations.

- CSCuh78336

  Symptom: %SCHED-2-EDISMSCRIT: Critical/high priority process ATM OAM Input may not dismiss. -Process= "ATM OAM Input", ipl= 0, pid= 128

  Conditions: ASR1006 running IOS XE RLS3.5.2 and higher, during execution of command "ping atm ..." on a looped VC.

  Workaround: There is no workaround.

- CSCuh87017

  Symptom: Hw-Sw: ASR1004 ASR1000-RP2 ASR1000-ESP20 asr1000rp2-adventerprisek9.03.09.01.S.153-2.S1 The ESP goes down logging messages similar to what is shown below: `Jun 27 19:59:12.308: %CPPHA-3-FAULT: F0: cpp_ha: CPP:0.0 desc:CPP Client process failed: cpp_cp det:HA class:CLIENT_SW sev:FATAL id:1 cppstate:RUNNING res:UNKNOWN flags:0x0 cdmflags:0x0 Jun 27 19:59:12.393: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_ha: cpp_ha encountered an error -Traceback= 1#e1875e79d5b29fc4e498ecbc61cdf452 errmsg:F6DB000 2230 cpp_common_os:FF5A000 C330 cpp_common_os:FF5A000 C130 :10000000 6FA4 :10000000 12718 evlib:F435000 E3B8 evlib:F435000 10564 cpp_common_os:FF5A000 12FF8 :10000000 F108 c:E51F000 1E938 c:E51F000 1EAE0 Jun 27 19:59:13.054: %PMAN-3-PROCHOLDDOWN: F0: pman.sh: The process cpp_cp_svr has been helddown (rc 134) Jun 27 19:59:14.289: %PMAN-0-PROCFAILCRIT: F0: pvp.sh: A critical process cpp_cp_svr has failed (rc 134) Jun 27 19:59:18.422: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_ha: cpp_ha encountered an error -Traceback= 1#e1875e79d5b29fc4e498ecbc61cdf452 errmsg:F6DB000 2230 cpp_common_os:FF5A000 C330 cpp_common_os:FF5A000 C130 :10000000 6FA4 :10000000 12718 evlib:F435000 E3B8 evlib:F435000 10564 cpp_common_os:FF5A000 12FF8 :10000000 F108 c:E51F000 1E938 c:E51F000 1EAE0`

  Conditions: On issuing "sh ip nat trans" when there are a large number of static networks translations the ESP may reset with the above messages. The issue is caused by a calculation dealing with the number of static network translations that are configured. It is possible to avoid this issue by moving out of the impacted range of static network translations (see workaround).

  Workaround: Determine the number of static network translations: `Router#$show platform hardware qfp active feature nat datapath stats | include static net non_extended XXXX entry_timeouts XXXX statics XXXX static net 126 hits XXXX misses XXXX` Take the number of static network translations ("static net") and divide it by 32, and then look at the remainder: `126/32 = 3 remainder 30` If the remainder is 30 or 31 this issue could be encountered when the 'show ip nat translation' is executed. To avoid this situation add or remove one or two static network translations, for example: `ip nat inside source static network X.X.X.X Y.Y.Y.Y /ZZ ip nat inside source static network A.A.A.A B.B.B.B /CC` The addresses used in these two static network translations do not need to be hit by any traffic, and do not need to be subnets that are regularly used within the network. Next verify that the remainder is no longer 30 or 31: `Router#$show platform hardware qfp active feature nat datapath stats | include static net non_extended XXXX entry_timeouts XXXX statics XXXX static net 128 hits XXXX misses XXXX 128/32 = 4 remainder 0` This can also be accomplished by removing one or two static network translations to lower the remainder.

- CSCuh90658

  Symptom: QFP crash.

Conditions: 1, create normal GTPv1 session and primary PDP 2, delete request with teardown false 3, update QOS with diff data TEID at both SGSN/GGSN, crash happened

Workaround: There is no workaround.

- CSCui19103

  Symptom: It is observed that no value is returned for an SNMP query (nhrpServerEntry) made by the SNMP server to the UUT (DMVPN Hub) in a Hierarchical DMVPN Scenario, where the HUB is an intermediate device which works as both DMVPN Hub and Spoke.

  Conditions: It is observed that no value is returned for an SNMP query (nhrpServerEntry) made by the SNMP server to the UUT (DMVPN Hub) in a Hierarchical DMVPN Scenario, where the HUB is an intermediate device which works as both DMVPN Hub and Spoke.

  Workaround: There is no workaround.

- CSCui32105

  Symptom: Symptom: In rare occasions the standby RP on a dual RP system may crash after performing a switchover.

  Conditions: This symptom occurs when an invalid message is sent from the RP to the RRP.

  Workaround: There is no workaround.

  Symptom: In rare occasions the standby RP on a dual RP system may crash after performing a switchover. The crash occurs due to an invalid message being sent from the RP to the RRP. The following tracebacks may be observed: `Jul 22 15:12:50.058 UTC: %COMMON_FIB-3-FIB_PATH_LIST_DB: Attempt to add empty path list 0/0: 7F0356E75750 -Traceback= 1#f7cffe13a57f1f88eefbd82deeaab4af :400000 876363 :400000 2C3B063 :400000 2C3AEA9 :400000 2C3CE05 :400000 2C2E3FF :400000 1728B37 :400000 1727E94 :400000 1727A77 :400000 1727968 :400000 5E1FF6F :400000 6536C5D :400000 5E1A433 :400000 5E1A09F Jul 22 15:12:50.062 UTC: %FRR_OCE-3-GENERAL: try to delete unempty frr db_node. -Traceback= 1#f7cffe13a57f1f88eefbd82deeaab4af :400000 876363 :400000 2CDF48D :400000 2CDD509 :400000 16CA2BD :400000 16CA21A :400000 171C2EC :400000 3EB784A :400000 1729863 :400000 1728B46 :400000 1727E94 :400000 1727A77 :400000 1727968 :400000 5E1FF6F :400000 6536C5D :400000 5E1A433 :400000 5E1A09F Jul 22 15:12:50.065 UTC: %FRR_OCE-3-INVALIDPAR: invalid setup state -Traceback= 1#f7cffe13a57f1f88eefbd82deeaab4af :400000 876363 :400000 2CDD520 :400000 16CA2BD :400000 16CA21A :400000 171C2EC :400000 3EB784A :400000 1729863 :400000 1728B46 :400000 1727E94 :400000 1727A77 :400000 1727968 :400000 5E1FF6F :400000 6536C5D :400000 5E1A433 :400000 5E1A09F`

  Conditions: There exists a very small timing window where the MPLS forwarding infrastructure may send an invalid message to the standby RP. The condition may occur if a large number of L2VPN AToM pseudowires are flapped within a window at the same time as a RP switchover is performed.

  Workaround: There is no workaround.

- CSCui43804

  Symptom: Traceback seen at ace_crypto_free_hw_spi.

  Conditions: Under load using static VTI.

  Workaround: There is no known workaround.

- CSCui48776

Symptom: The C/A LED on SPA-4xOC3-POS-V2 card comes up as amber after router reload. There is no alarms present on the controllers. No matter what you do, like remove/ insert the cable, or shut/ no shut the interface, once the interface comes back up the C/A light will be amber.

Conditions: The issue is seen after router reload or when "hw-module subslot x/y shutdown" and then "no hw-module subslot x/y shutdown" is issued.

Workaround: In order to fix it: Let the interface as is that means up/up. Do not administratively shutdown the interface. hw-module subslot x/y shutdown Remove the cable. no hw-module subslot x/y shutdown When the LED's are on (C/A will be amber), put the cable back in into the port. The C/A light glow green.

- CSCui90139

  Symptom: ASR1K : Crypto Route not getting deleted on Responder.

  Conditions: ASR1K : Crypto Route not getting deleted on Responder.

  Workaround: There is no workaround.

- CSCuj09925

  Symptom: In a PPPoE dual-stack environment, the Delegated-IPv6-Prefix is not sent to the start accounting record. The Delegated-IPv6 Prefix is logged only in the next Interim record, but this can take a long time depending on the configured update period

  Conditions: Delegated prefix allocated from an IPv6 pool which is configured via Cisco-AVPair "ipv6:delegated-ipv6-pool" in the RADIUS server.

  Workaround: There is no workaround.

- CSCuj44262

  Symptom: The 10GigE port is not up even though the XFP transmits laser.

  Conditions: This symptom occurs under the following

  Conditions: - Using SPA-1X10GE-L-V2 and XFP-10G-MM-SR. - Leaving the interface in shutdown state for a long time (over 6hrs).

  Workaround: Reload the SPA.

  Symptom: 10GigE port doesn't bring up though the XFP is transmitting laser.

  Conditions: - Using SPA-1X10GE-L-V2 and XFP-10G-MM-SR, - Leaving the interface in shutdown state for long time, say over 6hrs.

  Workaround: There is no workaround., but once hitting this symptom, reloading the SPA will fix the problem.

- CSCuj57479

  Symptom: Static Pat entries dont work and do not show up in the show ip nat translations output

  Conditions: when using both TCP and UDP port on the physical interface in the static pat config

  Workaround: instead of specifying interface x overload, use the ip address of the Interface. For example, ip nat inside source static tcp 10.1.1.1 6666 interface gig 0/1 56666 use this ip nat inside source static udp 10.1.1.1 6666 192.168.1.1 56666 (192.168.1.1 is the interface ip itself)

- CSCuj69001

  Symptom: Crash after adding the ACL with the ttl option to QoS policy

  Conditions: Create a policy with ACL containing ttl option. AND Attach this policy to an interface AND Send non-ip traffic (mpls or l2) to this interface. This has been seen on ASR1002 running asr1000rp1-advipservicesk9.03.06.00.S.152-2.S after adding the following: permit icmp host x.x.x.x host x.x.x.x ttl gt 20

Workaround: Don't use an ACL with ttl option in QoS policy. Or, add an IPv6 class-map to QoS policy. Example: Ipv6 access-list v6_acl Permit ipv6 any any Class-map match-any v6_class. Add this class to QoS policy. Match access-group name v6_class.

- CSCuj82693

  Symptom: ESPs going offline and remaining in "disconnecting" state for a few minutes, until fman_fp and cppc_cp processes failures.

  Conditions: %CPPBQS-3-QMOVESTUCK: Fx: cpp_cp: QFP 0 schedule xxx queue move operation is not progressing as expected

  Workaround: There is no workaround.

- CSCul14769

  Affected image:- 3.4.0aS, 3.7.3

  Symptom: -While upgrading/downgrading the image ssh ver is getting changed to 1 from 2. Due to this there is loss connectivity on SSH window.

  Conditions: SSH should be enabled on device with configured version 2 "ip ssh version 2"

  Workaround: (config)#crypto key generate rsa label SSHRSAKEYS (config)# ip ssh rsa key-pair SSHRSAKEYS Then do ISSU upgrade and manual downgrade, issue will not be seen.

  SSH is somehow receiving key size from crypto engine which is less than 768 bits so it is initializing SSH with version 1 but there is no keys present on the box which is less than 768 bits. SSH/PKI/ Crypto team is still investigating the problem. but with work-around mentioned by me is working properly. <IPNGN-AS>:With this WA config on the box, I observed rsa keys getting deleted even though the config was ssh ver 2. Here we cannot guarantee the WA was 100% because on the 3rd try with WA, we saw RSA keys getting deleted and further testbed was kept in same state for further debugging by SSH/crypto team. Please refer the attached email(RE SSH ver changedrsa key deleted during upgradedowngrade 3.4.0 to 3.7.3 vice versa.msg)

- CSCul17693

  Symptom: On the ASR1000 platform family, CISCO-ENHANCED-MEMPOOL-MIB & CISCO-MEMORY-POOL-MIB show lsmpi_io pool with little free memory. As a result, various SNMP management software applications may generate an error/notification.

  Conditions: This condition is shown from the moment the router boots up. The lsmpi_io pool is used on the Route Processor of all ASR1000 routers. Unlike other IOS versions IOSd on the ASR is a process running on IOS XE. IOSd has a single logical interface which communicates to IOS XE. This interface is called the Linux Shared Memory Punt Interface (LSMPI). When the ASR1000 boots the lsmpi_io pool is created and nearly all of the memory is allocated up front by design. Therefore, the little free memory shown in the MIBs is by design and does not indicate an error condition. The LSMPI interface is described further in this document: http://tools.cisco.com/squish/b64AB

  Workaround: There is no workaround for the lsmpi_io pool having little free memory. If some other piece of software is generating alarms for this reason the management software needs to be adjusted.

- CSCul26686

  Symptom: Scaled vlan qinq config on SPA. If the TCAM of SPA becomes full and more qinq vlan is configured then TCAM_VLAN_TABLE_FULL message is not displayed.

  Conditions: TCAM is full.

  Workaround: For verification whether a new entry has been added or not, check for TCAM entry using CLI on SPA console.

- CSCul33598

Symptom: On a dual RP system such as ASR1006 and ASR1013 standby RP polls for power supply sensors along with local environment sensors.

Conditions: An ASR router with dual RPs.

Workaround: There is no workaround.

- CSCul33952

  Symptom: FTP file-transfers running very slowly when source interface is management interface due to excessive check-sum failures.

  Conditions: source-interface for the ftp file-transfer is management ethernet interface.

  Workaround: There is no workaround.

- CSCul37689

  Symptom: With 76xx, customer associates more service instances of each access point to the same bridge domain to create a point to point local switching. Mac-learning in the bridge domain is disabled and therefore NOT limited by number of MAC addresses used. For asr1k is expected to implement same behavior under this feature.

  Conditions: None.

  Workaround: There is no workaround.

- CSCul49852

  Symptom: A router might see PPPoE-sessions in status WAITING_FOR_STATS (or WT_ST).

  Conditions: The system is configured as BRAS aggregating PPPoEoA or -oE-sessions. The issue was seen for just specific users or possibly because of using a specific profile or service like ShellMaps and Radius.

  Workaround: There is no workaround.

- CSCul56207

  Symptom: A standby RP crashes.

  Conditions: This symptom is seen on a Cisco ASR 1000 router used for PPPoEoA-aggregation when configuring a range/pvc. It was seen together with the following error message: asr(config-if-atm-range)pvc-in-range 10/45 %ERROR: Standby doesn't support this command ^ % Invalid input detected at '^' marker.

  Workaround: There is no workaround.

  Symptom: A StbyRP might see a crash.

  Conditions: his was seen on an ASR 1000 used for PPPoEoA-aggregation when configuring a range/pvc. It was seen together with the following error-message: asr(config-if-atm-range)pvc-in-range 10/45 %ERROR: Standby doesn't support this command ^ % Invalid input detected at '^' marker.

  Workaround: There is no workaround.

- CSCul65858

  Symptom: GARP for the NAT-inside-global-address is sent from a non-Active HSRP router. The problem is seen when one of the redundancy pair is reloaded and the interface comes up. Because of the behavior, traffic loss is seen on the NAT traffic. When receiving the GARP, active router shows the duplicate address message like below. %IP-4-DUPADDR: Duplicate address x.x.x.x on GigabitEthernetx/x/x, sourced by xxxx.xxxx.xxxx

  Conditions: The problem is seen on ASR1K platforms

  Workaround: There is no workaround.

- CSCul67817

  Symptom: max nat translations with ACL not working

  Conditions: With PAT mapping using ACL nat limit config

  Workaround: There is no workaround.

- CSCul68223

  Symptom: We saw RP CPU Spike using ASR1001/3.7.4S from "monitor platform software process rp active". The config is very simple(the default config, almost). When the CPU is high, the value is about 30-40%.

  Conditions: None.

  Workaround: There is no workaround.

- CSCul87051

  Symptom: ASR1k running 3.7.2S Two inside global addresses for the same inside local address. Sufficient pool to handle one-to-one translations

  Conditions: IPv4 nat - ip nat inside source route-map <route-map> pool <pool> reversible SIP traffic

  Workaround: There is no workaround.

- CSCum02221

  Symptom: Memory Corruption crash: chunk from bgp_attrlist_chunks accessed past redzone. With BGP debug update turned on there will be messages about wrong attributes, etc. by BGP Error Handling shortly before the crash.

  Conditions: This symptom is observed while running BGPv4 codenomicon suite; BGP receives an update with repeating valid attributes with flag lengths bigger than data in the packet. Crash will happen every time with a generic BGP session if update as described above is received, however under normal working conditions crash will not occur as above update is not valid.

  Workaround: There is no workaround.

- CSCum13378

  Symptom: An ASR1K configured as an IPSec endpoint may fail to reassemble fragmented ESP packets . During this failure state, the router will also log %ATTN-3-SYNC_TIMEOUT errors.

  Conditions: UDP packet of a specific size received on the clear side of the ASR is known to trigger this issue.

  Workaround: Use software crypto for large packets received on the clear side by configuring post-frag encryption - crypto ipsec fragmentation after-encryption. This will prevent the ASR from getting into the ATTN_SYNC state.

- CSCum25232

  Symptom: ASR1K will fail to verify a message that is signed using a non-standard RSA key length (2024 for example). The failure is commonly seen during SCEP enrollment or when validating a peer certificate when RSA-SIG is used for phase 1 authentication.

  Conditions: The failure has been observed on ASRs using an integrated ESP

  Workaround: There is no workaround.

- CSCum27365

  Symptom: Resource leak unexpectedly occurs when the “show logging persistent” command is executed. As a result, several commands such as “dir nvram:” fail when there are no resources available due to resource leak.

Conditions: "show logging persistent" command is executed.

Workaround: There is no workaround.

- CSCum46475

  Symptom: ATM VC object pending in AON BRAA04-asr#show platform software object-manager f0 pending-ack-update Update identifier: 477862718 Object identifier: 227150073 Description: `ATM PVC at ATM1/2/1.1, VCD 528, FCID 55163, Hw-FCID 65535, state 0x40608, dirty 0x0 Number of retries: 0 Number of batch begin retries: 0 asr#show platform software object-manager f0 object 227150073 Object identifier: 227150073 Description: ATM PVC at ATM1/2/1.1, VCD 528, FCID 55163, Hw-FCID 65535, state 0x40608, dirty 0x0 Status: Pending-acknowledgement, Epoch: 0, Client data: 0x13d55170 Issued action Update identifier: 477862718, Batch identifier: 0 Batch type: unknown Action: Create`

  Conditions: None

  Workaround: There is no workaround.

- CSCum69887

  Symptom: NAT cann't handle the tcp sequence properly with LDAP ALG after pdu size changed. NAT will not handle the delta value for the right ack message but thereafter messages, which may cause mis-acked message flows between two endpoints.

  Conditions: Send LDAP traffic with empty comment item in LDAP ALG.

  Workaround: There is no workaround.

- CSCum70828

  Symptom: SNMP Query on dot3StatsDuplexStatus is shown as unknown on SPA-5X1GE-V2.

  Conditions: While testing Ether-like MIB for SPA-5X1GE-V2.

  Workaround: There is no workaround.

- CSCum73080

  Symptom: Traceback seen while doing a 'default range' on the control, data and InterLink interfaces on a RG Active Router

  Conditions: Stateful HTTP / FTP traffic was being sent through the router.

  Workaround: Do a default on all the interfaces one by one instead of doing 'default range Gig x - y'

- CSCun13772

  Symptom: CPUHOG messages and watchdog timeout crashes are observed on an ASR1000 series router running DMVPN.

  Conditions: This has been observed on a router with a very large NHRP table (10-20k individual entries) with a very high number (thousands) of child entries per parent entry.

  Workaround: Reduce the number of child entries per parent entry through the use of supernetting.

- CSCun13999

  Symptom: Under interface superscription condition we might see the following error message on router console: %CMCC-3-PLIM_STATUS: SIP0: cmcc: A PLIM driver informational error TXMC0 - txmcBufferOverflow, block 1f count c8

  Conditions: When "fair-queue" is used in QoS policy-map, under interface subscription condition the flow-control between BQS and SPA might excommunicate, hence the error message is printed. %CMCC-3-PLIM_STATUS: SIP0: cmcc: A PLIM driver informational error TXMC0 - txmcBufferOverflow, block 1f count c8

Workaround: There is no workaround.

- CSCun20274

  Symptom: Standy RP source is not participating in clocking selection

  Conditions: Stanby RP bits must be configured

  Workaround: Remove and re-apply the stby-network-clk Source with different framing.

- CSCun20279

  Symptom: At uRPF loose mode, the suppress drop counter on ASR1K will count packets even in case the packets are symmetric flow. ASR1K should not count symmetric flow packets as sdrop at uRPF loose mode.

  Conditions: uRPF loose mode

  Workaround: There is no workaround. This ddts does not have any service/traffic impact.

- CSCun24809

  Symptom: An ASR router may reload and come up with the last reload reason being printed as watchdog. There will be a kernel core file generated in the harddisk/bootflash.

  Conditions: ASR router running IOS XE in a production environment,

  Workaround: There is no workaround.

- CSCun24965

  Symptom: On the ASR1000 series router hen configuring a QoS service policy using the service-fragment type, the shaping value is not correct.

  Conditions: A QoS Service Policy is applied using the service-fragment keyword, the shaped value is not correct.

  Workaround: There is no workaround.

- CSCun25536

  Symptom: Cmand core file is generated when ISSU subpkg upgrade is performed on a single RP system such as 4RU.

  Conditions: ISSU subpkg upgrade is performed on an RP on a single RP scenatio

  Workaround: There is no workaround.. System should come up fine on next reboot.

- CSCun27977

  Symptom: The following tracebacks appear : *Feb 21 01:10:29.603 PST: %SPA_CHOC_DSX-3-HDLC_CTRL_ERR: SIP1/2: SPA 1/2: 2 TX Chnl Queue Overflow events on HDLC Controller were encountered. *Feb 21 01:42:29.275 PST: %SPA_CHOC_DSX-3-HDLC_CTRL_ERR: SIP1/2: SPA 1/2: 3 TX Chnl Queue Overflow events on HDLC Controller were encountered.

  Conditions: There must be a back to back CT3 connection and policy related configs mentioned in enclosures config-frf12-Q1.txt and config-frf12-Q2.txt are copied to the running configs of first and second router respectively.

  Workaround: There is no workaround.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.5S

This section documents resolved issues on Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.5S.

- CSCtf46011

  Symptom: With c3845 gateway, insert mgcp gateway and one MGCP PRI, one MGCP CAS port, when resetting mgcp gw and PRI/CAS ports, or change device pool of MGCP PRI port, the MGCP PRI port will be in Unregister status. The call from/to this port will fail.

  Conditions: Not all the mgcp gateway has the issue. Only one hit the problem.

  Workaround: Click the MGCP PRI port and do reset. Further Information: This issue is cosmetic. GW sends RSIP(forced) and RSIP (restart) without CUCM ack to the first RSIP (forced). The first and second events are processed. Within CUCM Realtime Information System (RIS) when child (12) was created, it creates PerfMon counter object that have the same name as the object created by child(11). This operation failed because child(11) has not stopped and the same named object is still in use by child(11). When child(11) stops it deletes the PerfMon counter object for this port. As a result, the GUI is showing device unregistered. The device is actually registered but the GUI has a pointer for an old perfmon instance for this device. The device is currently registered and perfmon will show it registered under new instance.

- CSCtk05154

  Symptom: Not all dtmf is detected by the receiving endpoint. PCM analysis will show two tones too close together to be detected as two.

  Conditions: Dial the same number rapidly. For example 99999999.

  Workaround: There is no workaround.

- CSCtr82557

  Symptom: NHRP route watch debug messages are still printed even after all the debugs are turned off and should stop.

  Conditions: All NHRP debugs are turned on using "debug dmvpn detail nhrp" or "debug dmvpn all <all/nhrp>". This results in enabling NHRP route watch debugs as well. "undebug all" does not turn off NHRP route watch debugs.

  Workaround: Issue "no debug dmvpn all nhrp" even after issuing "undebug all".

- CSCua02200

  Symptom: LACP PDU not being punted to platform. And addition/removal of port-channel member link which is in UP state but port-channel is down due to min-bundle failure.

  Conditions: min-bundle failure on port-channel.

  Workaround: Adding links as a member to port-channel will resolve this issue.

- CSCua10797

  Symptom: Traffic is dropped instead of being sent in clear text when permit is configured on the KS and local deny on the GM.

  Conditions: Configure permit access list on KS and on GM configure a deny access list locally.

  Workaround: There is no workaround.

- CSCua73834

Symptom: IOS CA issues incorrect rollover identity certificates to its clients; the rollover certificates issued will have an expiry date corresponding to the end-date of the currently active (and soon to expire) CA certificate. Thus, the rollover identity certificate will not be valid after the CA rollover takes place.

Conditions: The issue is seen only if the clients have sent the rollover certificate request via an IOS RA certificate server.

Workaround: There is no workaround.

- CSCub06288

  Symptom: TSi Source address is not substituted with IKE local address at the responder during CREATE_CHILD_SA exchange to establish new IPsec SAs.

  Conditions: The initiator should be behind a NAT device and NAT-Traversal should occur in transport mode.

  Workaround: Establish IPsec SA's with IKE_AUTH exchange itself.

- CSCub14611

  Symptom: %IOSXE-3-PLATFORM: R0/0: kernel: physmap-flash.0: Chip not ready.

  Conditions: While doing redundancy force-switchover on ASR1006 (RP1).

  Workaround: Reload ASR1006.

- CSCub38910

  Symptom: COOP failure messages seen continuously on stby RP.

  Conditions: Seen on HA setup, there is no harm to the actual functionality nor the messaging to syslog as functionality is not yet present (except for the extra messaging). This is simple an erroneous messaging item.

  Workaround There is no workaround.

- CSCub41070

  Symptom: Punt Dropped packet Counter does not increment past max value.

  Conditions: None.

  Workaround: There is no workaround.

- CSCuc30309

  Symptom: Experiencing memory leak in IPSEC background process particularly in session_request_background.

  Conditions: Memory leaks were observed at the said function upon bringing up and clearing down sessions repeatedly in a DMVPN scale setup (without routing protocols).

  Workaround: Reload the router over a period of time.

- CSCuc41243

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

  Conditions: PfR BR session flap under session condition, not likely to reproduce in the lab.

  Workaround: There is no workaround.

- CSCud21267

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

  Conditions: Systems with dual RPs.

Workaround: There is no workaround.

- CSCud63146

  Symptoms: In a GETVPN scenario, the GM fails to install policies on reload. A crypto map is applied on ethernet 0/0 while the local address of the crypto map is configured with ethernet 0/1.1

  Conditions: This symptom occurs after a reload. The GM fails to install policies from the key server.

  Workaround: Remove the crypto map configuration on the interface and reapply.

- CSCud69110

  Symptom: IKE_CP_ATTR_SPLIT_EXCLUDE support is needed on IOS side for anyconnect client.

  Conditions: - include-local-lan

  Workaround: There is no workaround.

- CSCue43682

  Symptom: Transcoding sessions are intermittently becoming stuck after call is cleared.

  Conditions: When transcoding configured in DSPfarm.

  Workaround: Reload Gateway.

- CSCue56272

  Symptoms: The Cisco ISR crashes due to watchdog timeout after SYS-3-CPUHOG errors with a traceback.

  Conditions: This symptom is observed with voice traffic through the router.

  Workaround: There is no workaround.

- CSCue74977

  Symptom: Route not found on UUT for RRI testcases .

  Conditions: When the testcase for RRI, reverse-route remote-peer 16.0.0.1 gateway is checked, route is not found on the router.

  Workaround: There is no wrokaround.

- CSCue94576

  Symptom: Both outgoing RTP streams are dropped on the router interface. When looking into output, both incoming and outgoing RTP streams are clearly visible, however packet capture from the interface contains only two incoming RTP streams. And, the router console presents the following error message: `IP-3-LOOPPAK Looping packet detected and dropped - src=172.22.233.65, dst=172.22.233.76, hl=20, tl=200, prot=17, sport=16390, dport=20832 in=GigabitEthernet0/1, nexthop=172.22.233.76, out=GigabitEthernet0/1 options=none -Process= "IP Input", ipl= 0, pid= 126 -Traceback= 21127EC4z 21129118z 2112A560z 2112AA38z 2112AFA4z 21110178z 2112C580z 21110918z 21110B58z 21110C38z 21110E50z 23C1ACA4z 23C1AC88z`

  Conditions: Defect was encountered in 2900 series routers with IOS version: 15.2-3.T2 when using "no ip cef" command.

  Workaround: Issue the "ip cef" command.

- CSCuf04726

  Symptom: IPsec (crypto-map mode) configured, manually disable VFR, after reload, the "no ip virtual-reassembly-out" CLI is lost, VFR is re-enabled.

Conditions: 1) Apply crypto map on the interface 2) Manually disable vfr "no ip virual-reassembly-out" 3) Save config 4)reload after reload . The "no ip virual-reassembly-out" is lost, VFR is reenabled.

Workaround: After reload, need to manually disable vfr "no ip virual-reassembly-out".

- CSCuf52420

  Symptom: A PPP link flap may be seen on an ASR1000 router performing an RP switchover.

  Conditions: This behaviour may be seen with POS interfaces configured with PPP encapsulation. The flap may be seen after an RP switchover. The link typically recovers soon afterwards.

  Workaround: There is no known workaround for this behaviour.

- CSCuf74026

  Symptom: When the ipsec lifetime is changed globally it does not take effect on the ipsec session.

  Conditions: Any ipsec implementation with ipsec profile.

  Workaround: unconfigure the lifetime from the ipsec profile.

- CSCuf82417

  Symptom : When an IPv6 ACL is defined with 'remark' on the Key-server, the Key-server is translating this entry as "deny ipv6 any any" before pushing it in TEK to the GM. Due to this the GM is installing this as the first sequence in its temporary downloaded acl and any v6 dataplane traffic that should have been encrypted goes out as clear-text bypassing the crypto.

  Conditions : Seen on ASR1K (ASR1002x) acting as Keyserver where the IPv6 ACL is defined, running the latest MCP_DEV code. This can be service impacting, as usually customers have remarks in their ACL's which helps them identify the ACL per group/customer/..etc and for better readability.

  Workaround : Do not configure the IPv6-ACL with the 'remark' statement.

- CSCuf93460

  Symptom: Certain PKI CLIs may show wrong values.

  Conditions: First found on IOS 15.1(4)M6 but not exclusive to it.

  Workaround: There is no workaround.

- CSCug11093

  Symptom: Observed the log SCOOBY-3-SERIAL_BRIDGE_CRITICAL_ERROR: F1: cman_fp: Reloading F1:0 due critical event 0x80000 in block epi/0 of serial bridge 0.

  Conditions: When FP100 is deployed. The rare event was seen once in two years after FP100 was shipped.

  Workaround: There is no workaround.

- CSCug14423

  Symptom: A packet gets dropped when a spoke-spoke session is triggered in Dynamic Multipoint VPN (DMVPN).

  Conditions: This symptom occurs when a ping is sent using a tunnel interface as the source or the destination.

  Workaround: Send traffic from host-host.

- CSCug37057

  Symptom: RSVP hello stays in "PASSIVE".

Conditions: Ospf send bdb packet error for incomplete adj.

Workaround: There is no workaround.

- CSCug65080

  Symptom: Experiencing memory leak in Crypto Route Q process particularly in ikmp_config_route_send_to_ipsec.

  Conditions: When running 7301 router and connecting EasyVPN through it, causes leak in Crypto Route Q process over time.

  Workaround: Reload the router over a period of time.

- CSCug78227

  Symptom: ASR1001-5-DEV(config-sbc-sbe-sip-hdr-ele)# sip header-profile hprof2 ASR1001-5-DEV(config-sbc-sbe-sip-hdr)# store-rule entry 1 ASR1001-5-DEV(config-sbc-sbe-sip-hdr-ele-act)# condition request-uri sip-uri-user store-as uname Error: sip-uri-user is only valid for To, From and Request-Line

  Conditions: This happens if following config is paste into config terminal or on reading startup-config with following config:

```
-------------------------------------------------------------------------------
-----------    sip header-profile hprof1     store-rule entry 1      condition header-
name Allow header-value store-as Avalue     store-rule entry 2      condition request-
uri sip-uri-user store-as uname
```

  Workaround: Exit sbc and re-enter the specified store-rule/condition:

```
-------------------------------------------------------------------------------
-----------    sip header-profile hprof1     store-rule entry 1      condition header-
name Allow header-value store-as Avalue      exit     exit    exit   exit  sbc test
sbe    sip header-profile hprof1      store-rule entry 2       condition request-uri
sip-uri-user store-as uname
```

- CSCug81308

  Symptom: ESP200 continuous crash with egress service policy on scaled VLAN.

  Conditions: Have multiple vlan scaled in router with ESP200 in the FP slot.

  Workaround: There is no workaround.

- CSCuh27266

  Symptom: CPP core not generated when FP crash happens.

  Conditions: Perform SPA OIR with Unicast/Multicast/Broadcast storm control on 32k EFPs .

  Workaround: There is no workaround.

- CSCuh27343

  Symptom: A CUBE router may reload.

  Conditions: This is only seen on a router processing voice traffic with CPA feature enabled.

  Workaround: There is no workaround.

- CSCuh35993

  Symptom: Create an RRI route for deny ACL lines in the crypto map.

  Conditions: 15.x code and L2L ipsec tunnel.

  Workaround: There is no workaround.

- CSCuh57439

Symptom: The router reloads due to heap memory exception such as "FREEFREE" or "BADMAGIC" within the checkheaps process.

Conditions: The router has experienced heavy, likely prolonged voice traffic, especially CUBE (IP-IP gateway) calls.

Workaround: There is no workaround.

- CSCuh63727

  Symptom: Router may crash when unconfiguring large (8k) redirect ACL list in MASK config.

  Conditions: None.

  Workaround: There is no workaround.

- CSCuh78055

  Symptom: MN-BITS IN stays in Locked state even when MN-BITS OUT is removed.

  Conditions: MN-BITS IN stays in Locked state even when MN-BITS OUT is removed.

  Workaround: There is no workaround. But as corrective action, removing and re-applying input source will bring the falsey BITS_IN source to QL-FAILED state; then automatically sync source is shifted to next best available.

- CSCuh80368

  Symptom: erspan performance downgrade in FP160.

  Conditions: erspan under FP160.

  Workaround: There is no workaround.

- CSCuh87919

  Symptom: Seeing PuntPerCausePolicerDrops on sending traffic through LISP router.

  Conditions: No traffic drops associated.

  Workaround: There is no workaround.

- CSCuh88723

  Symptom: Plim Ingress classification doesn't work on Clearchannel-SPAs. High priority traffic will continue to be treated as normal traffic and flows in Low Priority queue.

  Conditions: With PLIM ingress classification, despite assigning "map ip dscp 16 - 31 queue strict-priority" traffic flows in Low Priority queue.

  Workaround: There is no workaround.

- CSCuh89946

  Symptom: Customer may see the following error messages: `%SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level %SYS-2-MALLOCFAIL: Memory allocation of 80 bytes failed from0x5CEEBCC, alignment 0 Pool: Processor Free: 196745624 Cause: Interrupt level allocation Alternate Pool: None Free: 0 Cause: Interrupt level allocation - Process= "<interrupt level>", ipl= 3, pid= 147 %IPMCAST_RPF-3-INTERNAL_ERROR: An internal error has occured while obtaining RPF information (No memory available to create pathinfo for RPF lookup)`

  Conditions: Unknown at this time. Additional information to follow.

  Workaround: There is no workaround.

- CSCuh91563

  Symptom: ucode crash seen on unconfiguring NAT with nbar.

  Conditions: Seen during a script run.

  Workaround: There is no workaround.

- CSCuh92837

  Symptom: When fax tones are detected in the early media phase of the call, the gateway does not initiate a fax mode switchover.

  Conditions: The call must establish early media, and fax tones must be detected in this phase of the call.

  Workaround: There is no workaround.

- CSCuh93572

  Symptom: Certain sequence of config/unconfig of PLIM comands resulted in error.

  Conditions: 1. Add DSCP based Plim config. 2. Mark certain DSCP value as high or low priority with PLIM config command. 3. Delete the config added in step 1. 4. Now try to add a TOS bases Plim config. It will through error stating "config done in step 2" must be deleted. But config in step 2 is a subset of config in step1. It should be enough if the config in step1 is removed to add any new plim config.

  Workaround: Remove the DSCP based config completely before adding any new TOS based config.

- CSCui01133

  Symptom: ATM autovc padi timeout.

  Conditions: autovc scaling.

  Workaround: There is no workaround.

- CSCui07002

  Symptom: When two routers attempt to build an IKE session and use PKI for authentication, if the CRL is/has expired, the responding router crashes and reloads.

  Conditions: This symptom is observed with PKI chain-validation, CRL check, and expired CRL.

  Workaround: Disable the CRL check.

- CSCui11009

  Symptom: "clear controller wanphy x/x/x" command cannot clear counters of "sh controller wanphy x/x/x". This issue is seen on ASR1006.

  Conditions: When insert the SPA after the router is up.

  Workaround: Reload the router with the SPA.

- CSCui12023

  Symptom: OIR of Metronome-spa_BITSOUT results in QL-DNU at connected input source (Metronome-spa/Kingpin BITSIN).

  Conditions: OIR of Metronome-spa_BITSOUT

  Workaround: Remove and Re-apply BITSOUT clocking configuration.

- CSCui14805

  Symptom: Dubious QL-SEC seen on 10M src of MN spa aftr cable removal, reloadng SPA

Conditions: GPS 10M port connected to Symmetricom device.

Workaround: Remove and Re-apply the config to go QL-FAILED state. network-clock input-source 3 External 2/0/0 10m

- CSCui17100

  Symptom: Ucode crash seen.

  Conditions: Crash seen when doing cc_oir with scaled EVC-EOMPLS config.

  Workaround: There is no workaround.

- CSCui22356

  Symptom: During Sub package ISSU Upgrade is performed on ASR1002-X router after upgrading the standby RP (R0/1) with new RP subpackages, Switchover is forced from the active IOS process to the standby IOS process. During the switchover, new active performs configuration Bulk-Sync with the standby. During this Bulk Sync operation, the configuration related to the Interfaces is not synced to the standby due to Bulk Sync MCL failures. The following error message will be displayed when this error is present. Sample Error Message: `<.............> Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check full list of mismatched commands via: show redundancy config-sync failures mcl Config Sync: Starting lines from MCL file: interface Tunnel150 ! <submode> "interface" - tunnel source GigabitEthernet0/0/0.34 <.............>` Standby takes more time(~744 seconds) for reaching terminal State.

  Conditions: The symptom is observed after redundancy force-switchover step in ISSU upgrade procedure.

  Workaround: Peform a standby IOS reload. "hw-module subslot R0/0 reload"

- CSCui37419

  Symptom: ASR1K CPP ucode crash.

  Conditions: Very big DNS packet are being processed.

  Workaround: There is no workaround.

- CSCui39989

  Symptom: PKI fails to validate (sub, peer) cert chain received from IKE.

  Conditions: PKI hierarchy: root -> sub -> peer - root and sub locally trusted - IKE profile configured with "ca trust-point sub" only - chain-validation from sub to root.

  Workaround: See CSCuh73796.

- CSCui42826

  Symptom: fman_fp crash seen with 1K tunnels and routemaps.

  Conditions: While sending traffic with 1K tunnels and routemaps with ipv6 ACL.

  Workaround: There is no workaround.

- CSCui53438

  Symptom: While busying out the isdn voice port gracefully, busyout functionality is not working as expected as serial interface goes down immediately.

  Conditions: Set the busyout monitor in the voice-port.

  Workaround: Removing the busyout monitor.

- CSCui54042

  Symptom: ASR 1004 Router crashes when running command "no crypto pki certificate pool"

Conditions: This has been seen on the ASR1004 running the following: asr1000rp2-advipservicesk9.03.07.03.S.152-4.S3 asr1000rp2-advipservicesk9.03.07.03.S.152-4.S2 asr1000rp2-advipservicesk9.03.07.03.S.152-4.S1

Workaround: Do not run the command "no crypto pki certificate pool"

- CSCui64796

  Symptom: cpp_cp_svr crash in LNS.

  Conditions: While tearing down PPPoX sessions. On ESP=100, ESP-200 or ASR1K 2RU VE systems, if more than 4000 sessiions are created on one interface and all sessions on that interface are torn down, this leads to a cpp_cp_svr crash on the ESP.

  Workaround: There is no workaround.

- CSCui72473

  Symptom: When the traffic is flowing through ATM1xOC3, the rate of flow fluctuates very fast and the counters do not match. The “sh int atm0/3/0 | i pack” command can be used repeatedly to check the rate.

  Conditions: The traffic should be flowing through ATM SPA.

  Workaround: There is no workaround.

- CSCui74020

  Symptom: After configuring cdp run ! interface gi0 dp enable on an ASR1K router, the router is not able to find its CDP neighbor (e.g. a Switch): `ASR1k# show cdp nei Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay Device ID Local Intrfce Holdtme Capability Platform Port ID` while the switch can find its CDP neighbor (ASR1k): `Switch#show cdp nei Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Device ID Local Intrfce Holdtme Capability Platform Port ID ASR1k Gig 1/0/19 134 R I ASR1006 Gig 0`

  Conditions: CDP enabled globally and on Mgmt Interface.

  Workaround: There is no workaround.

- CSCui74757

  Symptom: ESP crashes running 3.9.1 when NAT enabled.

  Conditions: Nat must be enabled.

  Workaround: There is no workaround.

- CSCui75391

  Symptom: Sometime there will not be any output for the command "show sbc global sbe sip subscribers filter <prefix>".

  Conditions: Observed on a Cisco ASR1k platform configured as CUBE using the Service Provider (SP) feature set running IOS-XE version 15.3(1)S2.

  Workaround: The command output is not granular enough. For example: If we execute command like this then it works: `#v1-z11#show sbc global sbe sip subscribers filter sip:1037@a.b.c.d #SBC Service "global" # #There are currently 2060 subscribers registered on this SBC. # #SIP subscribers: # #AOR: sip:1037@a.b.c.d #Subscriber Location[s]: sip:1037@x.x.x.x:5063 -> ENDPOINTS/PUBNET #`

```
Fast register active, fast time remaining 58 sec #Registrar adj:          SIPCORE
#Time left:              163 secs #Subscriber Category[s]: VRF Global IPv4 a.b.x.y
```
then we see expected information about "sip:1037@a.b.c.d" subscriber. But if we execute: `#v1-z11#show sbc global sbe sip subscribers filter sip:1037 #SBC Service "global"` we don't see anything. So the workaround is to use the first option.

- CSCui80542

  Symptom: Sending a PING to an IPv6 EID from a Proxy ITR without specifying the source interface can cause a crash which resets the FO.

  Conditions: When sending an ICMPv6 packet, we try to set the source UDP port, and depend on the source interface supplied in the exec command to do that. When the source interface is not included in the ping command, the source UDP port is invalid, and a crash ensues when LISP attempts to use it.

  Workaround: Include 'source <interface>' to ping commands on the Proxy ITR.

- CSCui80961

  Symptom: The output of the following command shows that the QM CPP DRAM increases but does not decrease when fair-queue is removed from a class before it is active in HW. **show plat hard qfp act inf exmem stat user | incl QM**. Over time the system runs out resource DRAM causing subsequent configuration events that require CPP DRAM objects to fail. The impact could be the system being unable to process new configuration events or the data plane being unable to allocate resource DRAM during packet processing.

  Conditions: When fair-queue is removed from a class before it is activated in the hardware, the BQS RM was not freeing the WRED DRAM object used to store the fair-queue configuration. Over time, the system runs out of CPP resource DRAM. The error message described in the description is displayed and all configurations start failing. This conditions impacts the whole system as opposed to just queueing features.

  Workaround: There is no workaround.

- CSCui84344

  Symptom: Outbound IPsec sequence numbering is not synced during HSRP failover.

  Conditions: This symptom is observed when an IPSec Stateful HA Solution is deployed on a set of 3900E devices running Cisco IOS Release 15.2(4)M4 and/or Cisco IOS Release 15.1(4)M6.

  Workaround: Disable IPSec Anti Reply check on the HA pair's remote peer(s).

- CSCui84532

  Symptom: RP is again fragmenting it.

  Conditions: Giant pkts are sent from SPA after LAF.

  Workaround: There is no workaround.

- CSCui88245

  Symptom: The CPP process could while adding fair-queue on the fly. This does not require scaling to occur.

  Conditions: When fair-queue is added on the fly while a default parent schedule is being deleted, a crash could occur because the RM cleanup code is destroying a wrong tree.

  Workaround: There is no workaround.

- CSCui90634

Symptom: If you attach a service which is not enabled to a interface, and then detach it, this will cause the service at index 0 in wccp cpp client be changed to unconfigured state. This bug may have the following symptoms: 1. The web-cache service works fine, but the counters of it will be incorrect. 2. If you then config a new service and make it active, like config service 61 and 62, web-cache service will not work anymore, because service 61 has overwrite the descriptor of web-cache in cpp_client. The packets that should be sent to client of web-cache will be sent to client of service 61 instead. 3. If web-cache is the only service, a traceback will appear, because wccp cpp client can't find any active descriptor, thus the periodic stats polling fails. 4. If change the properties of web-cache after step 2, a traceback will appear. 5. If you remove service 61 after step 4, with "no ip wccp 61" command, a traceback will appear.

Conditions: There are 3 cases of WCCP configuration: 1. WCCP service is configured on global & interface level. 2. WCCP service is configured on global level, but not configured on interface level. 3. WCCP service is not configured on global level, but configured on interface level. This issue is only triggered if unconfigure the service on interface in case 3. There is a special case which is less possible to occur can also trigger the issue: 1. WCCP service is configured on global & interface level. 2. Unconfigure the service on global level, and it remain configured on interface level. 3. Reload the router. 4. Unconfigure the service on interface level. In this case, after reload in step 3, It is the same as case 3. If there is no reload operation, every will be fine. commands: Ultra-WCCP1#conf t Ultra-WCCP1(config)#ip wccp web-cache Ultra-WCCP1(config)#interface gigabitEthernet 1.200 Ultra-WCCP1(config-subif)#ip wccp 23 redirect in Ultra-WCCP1(config-subif)#no ip wccp 23

Workaround: Enable service before attach it to an interface. If this problem has happened, a reload will solve this.

- CSCui96035

  Symptom: B2B RP crash.

  Conditions: None.

  Workaround: There is no workaround.

- CSCui96679

  Symptom: On a Cisco ASR1k running the Cisco CUBE SP (Service Provider) feature set, IOS-XE version 15.1(3)S1, it is sometimes observed that a specific call transfer will have no way audio (dead air) upon the transfer completion.

  Conditions: The CUBE SP has at least three physical interfaces that terminate three different SIP trunks (for example to ITSP, SIP based IVR and to a Cisco Callmanager) and the problematic transfer call flow signaling traverses all three SIP trunks on the same CUBE.

  Workaround: If you have more than one CUBE available and if one of the transfer call leg traverses this second CUBE then the problem is not observed.

- CSCuj01420

  Symptom: ESP ucode crash observed with a SIPvicious packet observed `%CPPHA-3-FAULT: F0: cpp_ha: CPP:0.0 desc:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR(interrupt) class:OTHER sev:FATAL id:2121 cppstate:RUNNING res:UNKNOWN flags:0x7 cdmflags:0x8`

  Conditions: The crashes are seen with SIPvicious packets.

  Workaround: Disable the SIP ALG for this port using **no ip nat service sip udp port 5060 no ip nat service sip tcp port 5060**

- CSCuj02519

  Symptom: Chunk memory leak in Crypto Proxy.

  Conditions: This is only seen with IPSEC HA configured.

Workaround: There is no workaround.

- CSCuj11301

  Symptom: Standby SBC ASR1k seeing "SNMP-3-INPUT_QFULL_ERR". SNMP input queue never drops, it continues to increase until it gets stuck at 1000, causing SNMP unresponsiveness to the device.

  Conditions: When polling ciscoSbcCallStatsMIB on Standby-RP ASR1k.

  Workaround: "default snmp-server" to soft reset the SNMP Engine to make the ASR1K respond again (refresh the input queue); then apply SNMPVIEW configuration to block the MIB. For example: `**********` `snmp-server view cutdown iso included snmp-server view cutdown ciscoSbcCallStatsMIB excluded snmp-server community <insert_your_community_string_here> view cutdown RO snmp-server community <insert_your_community_string_here> view cutdown RW` `**********`

- CSCuj12613

  Symptom: Duplicate digits received by 3rd party UA when RTP-NTE packets are sent from IOS SW MTP.

  Conditions: IOS SW MTP Originates RTP-NTE packets.

  Workaround: There is no workaround.

- CSCuj14019

  Symptom: %CMRP-3-UDI_AUTH: F0: cmand: Quack Unique Device Identifier authentication failed, show up.on ASR1001.

  Conditions: After reloading the box or inserting SFPs.

  Workaround: There is no workaround.

- CSCuj15540

  Symptom: Alignment errors reported on a router acting as a voice gateway.

  Conditions: This has been seen only on routers passing RTP packets.

  Workaround: There is no workaround.

- CSCuj21186

  Symptom: ESP5/ASR1001/ASR1002-F fails to come online during power hard reset.

  Conditions: ESP5 on ASR1k/ ASR1001 / ASR1002-F during system power up.

  Workaround: There is no workaround.

- CSCuj21502

  Symptom: show run only shows 191 na-dst-prefix-table out of 200.

  Conditions: Configured a lot of na-dst-prefix-table, specially, more than 191.

  Workaround: There is no workaround.

- CSCuj25418

  Symptom: The ESP-100 and ASR1K-2X crash when flat policies are applied on both the tunnel and the destination sub-interface. This issue is observed when QOS is applied first on the tunnel then on the sub-interface as follows: `policy-map tunnel-shaper class class-default shape aver per 20 policy-map sub-int-shaper class class-default shape ave per 90`. Be sure

the tunnel is active and pointing to the sub-interface with QoS applied before applying the sub-interface policy. See the attached repro-steps for details. `int tunnel1  service-policy out tunnel-shaper  int g2/3/0.100  service-policy out sub-int-shaper`

Conditions: When a sub-interface policy is applied after QoS is active on a tunnel, the tunnel is reparented from the current aggregation node to the sub-interface node. Since reparenting a leaf node requires adding a temporary node in the hierarchy to be able to move flow-control gracefully, the logic to detach the source leaf node from the temporary node was missing. As a result, the code generated a fatal error while attempting to free the temporary node before it is empty.

Workaround: There is no workaround.

- CSCuj30033

  Symptom: ATM interface - SPA-1XOC3-ATM-V2 - shows counters frozen when interface is shut down.

  Conditions: Running traffic over an ATM (SPA-1XOC3-ATM-V2) interface and then shutting down the interface - interface counters remain frozen and do not return to zero.

  Workaround:There is no workaround.

- CSCuj31165

  Symptom: crpcipSecGlobalActiveTunnels is incrementing endlessly.

  Conditions: crpcipSecGlobalActiveTunnels OID does not decrements when the current active tunnel is removed.

  Workaround: There is no workaround.

- CSCuj33901

  Symptom: ASR1000-RP2's actual ACTV/STBY LED state is incorrect. Although RP2 state is active, STBY LED light up. This issue is seen while using V04 RP2.

  Conditions: V04 RP2.

  Workaround: Please refer to Field Notice FN63704.

- CSCuj33916

  Symptom: For VC type 4 PW, Ethernet VLAN, with single dot1q header packet, if one configure rewrite pop 1, expected situation is to copy COS from this header into dummy tag. In reality, we hit a bug, when COS 0 is copied into dummy tag into CORE.

  Conditions: When transported traffic has outer vlan tag only, packet in MPLS core does not have copied priority field from dot1q header into MPLS EXP bits. Instead there is 0. When transported traffic has outer vlan tag and some vlan tags (QinQ) , packet in MPLS core does have copied priority field from outer dot1q header into MPLS EXP bits.

  Workaround: Configure input policy-map under service-instance, where each class match dot1Q COS and impose EXP bits. Further Problem Description:

- CSCuj39496

  Symptom: When configuring Input MPLS aware FNF (under interrface config --- mpls flow mon MON_NAME in) it can happen that FNF will cease to function due to cache entry leak/exhaustion.

  Conditions: This can only occur with Input MPLS FNF and moreover only will occur with certain labels. In particular it will occur for MPLS labels for which the output of show plat hard qfp active feature cef-mpls prefix mpls <LABEL NUM> does *not* have an IPV4 adjacency.

  Workaround: There really is no workaround other than to realize that this will only happen for 1. MPLS FNF 2. Input FNF (not Output FNF). 3. For MPLS labels that no not have the IPV4_ADJACENCY.

- CSCuj42585

  Symptom: When a flat policy is applied to a MLPPP, MFR or GEC aggregation bundle, the current leaf schedule object is replaced with a new one. The code was not updating the cached object which resulted in accessing invalid memory when the bundle bandwidth is updated. The bandwidth is updated when a member link is added to or removed from the bundle. Configuration example: `policy-map foo  class prec1  bandwidth percent 10  interface Port-channel1 aggregate  ip address 8.0.0.1 255.255.255.0  no negotiation auto  lacp min-bundle 2 service-policy output foo`

  Conditions: When a bundle schedule is replaced, the cached object was not being updated leading to interface bandwidth update event to access invalid memory. The problem is not easy to recreate as would require the QOS event for processing the flat policy to be interleaved with an interface bandwidth update event.

  Workaround: There is no workaround.

- CSCuj44868

  Symptom: Wrong traffic distribution after adding new class with fair-queue and bandwidth percent 15 to the existing policy on fly.

  Conditions: After adding new class with fair-queue and bandwidth percent 15 to the existing policy on fly.

  Workaround: There is no workaround.

- CSCuj45418

  Symptom: ASR1002-X reloads with the corefile reporting CIF_CSR32_CIF_CIF_MISC_GRP2_ERR_LEAF_INT__INT_CIF_EPIFC_CRC_ERR interrupt.

  Conditions: Only applies to ASR1002-X running IOS images prior to 15.2(4)S4a (XE3.7.4a). The issue is not specific to any configuration or traffic pattern.

  Workaround: There is no workaround.

- CSCuj47795

  Symptom: Anti-replay protection is disabled for Phase II IPSec SAs. A "show crypto ipsec sa" will show "replay detection support: N". Example: `Router#sh crypto ipsec sa | i trans|repl transform: esp-gcm 256 ,  replay detection support: N  transform: esp-gcm 256 , Router#`

  Conditions: IKEv2 is being used for negotiating Phase I SAs, and the Phase II transform set is configured to use either AES-GCM or AES-GMAC with any number (128, 192 or 256) of bits.

  Workaround: There is no workaround.

- CSCuj55267

  Symptom: cpp_cp_svr crash with model F QoS and multiple PPPoEoA/PPPoA VCs on one or more ATM PVPs.

  Conditions: While bringing up multiple PPPoEoA/PPPoA sessions with model F QoS on one or more ATM PVPs.

  Workaround: There is no workaround.

- CSCuj56505

  Symptom: SCCM phone registration on CCM via ASR1k is not happening.

  Conditions: ASR1k is configured with NAT configuration.

  Workaround: There is no workaround.

- CSCuj58272

  Symptom: The CP process crashes when reparenting more than 128 entries from one tree to the other. A reparenting event could be stimulated by either an internal or external event but this issue is more likely to caused by an internal reparenting. An internal reparenting could occur when a leaf node is transformed into a hierarchy layer node or when de-aggregating an aggregation node after the schedule size is below the 4000 threshold.

  Conditions: When reparenting either a leaf or hierarchy layer entries, the resource manager was not clearing the counter that tracks the number of entries that need to be flushed after processing the first batch. This caused the code to run incorrectly to a point of completing the request prior to reprogramming the HW correctly. As a result some entries may be left in the source parent which cause a crash when the tree is freed before it is empty.

  Workaround: There is no workaround.

- CSCuj61598

  Symptom: ASR1K cpp_cp_svr crash on ASR1002x or ASR1K using ESP100.

  Conditions: This issue has only been see on bundle type interfaces such as MLPPP, MLFR, GEC and possibly ATM if a hierarchical QoS policy is replaced with a flat QoS policy and then a rate change event occurs on the interface (such as removing or adding a link on a bundle type interface). The trigger is the bandwidth change following replacement of the hierarchical QoS policy with a flat QoS policy.

  Workaround: If a hierarchical QoS policy is replaced with a flat QoS policy this issue can be avoided by first deleting the bundle interface, adding it back, and then applying the flat QoS policy. Further Problem Description: As indicated above, this issue is specific to ASR1002x and ASR1K using an ESP100. This issue is not applicable to ASR1K using ESP5, ESP10, ESP20, or ESP40. This issue is also specific to the IOS XE release trains for XE3.7 15.2(4)S and later.

- CSCuj62858

  Symptom: Active NAT tables in a VRF are cleared unexpectedly when unconfiguring a static NAT belonged to other VRF.

  Conditions: The problem happens when following conditions are met. - 'network' option is used in the NAT rule. - The NAT rule which is to be unconfigured has overlapped local/global addresses with other NAT rules.

  Workaround: There is no workaround.

- CSCuj65437

  Symptom: PSTN ----- T1 PRI --- 2911 GW ---- h323 ---- CUCM --- Ip phone.

  In a scenario when the gateway receives two successive OLCs with the same mutlicast MOH address the gateway stops streaming MOH from the flash. When the first OLC comes to the gateway it streams multicast moh. Then for example if the caller transfers to a directed-park number in CUCM another OLC comes to the gateway with the same multicast ip address. The gateway should continue streaming MMOH. However no further moh is streamed and the PSTN user hears dead air.

  Conditions: This symptom is observed in Cisco IOS Releases 15.1(4)M6, 15.1(4)M7, 15.2(4)M5, and 15.3(3)M.

  Workaround: Downgrade the IOS to Cisco IOS Release 15.1(4)M4.

- CSCuj71839

  Symptom: CLI hang in SBC adjacency SIP mode.

  Conditions: This issue is observed when over 2000 sbc SIP adjacencies are configured.

  Workaround: There is no workaround.

- CSCuj74574

  Symptom: Router acting as a PKI client fails to delete its expired identity and CA certificates after it has rolled over. So, the output of "show crypto pki certificate" shows that the router has two sets of certificates: One set of identity and CA certificates that is current and valid. Another set of identity and CA certificates that is old and expired. Both sets of certificates are bound to the same trustpoint.

  Conditions: The issue is seen primarily when the client router has enrolled to an IOS CA via and IOS RA router.

  Workaround: There is no workaround. The old set of certificates get deleted eventually upon the next certificate renewal process initiated by the client router.

  An example of what is observed: `Router#sh crypto pki cert Time source is NTP, 16:18:12.777 UTC Tue Oct 8 2013 !--- Note the current time above. Certificate Status: Available Certificate Serial Number (hex): 0B Certificate Usage: General Purpose Issuer: cn=Root-CA ou=TAC o=Cisco c=IN Subject: Name: DMVPN-HUB1-NEW.cvo.IN.Cisco.Cisco Serial Number: XYZ1234567A serialNumber=XYZ1234567A hostname=DMVPN-HUB1-NEW.cvo.IN.Cisco.Cisco Validity Date: start date: 16:17:31 UTC Oct 8 2013 end date: 16:37:31 UTC Oct 8 2013 Associated Trustpoints: cvo-pki CA Certificate (Rollover) Status: Available Certificate Serial Number (hex): 09 Certificate Usage: Signature Issuer: cn=Root-CA ou=TAC o=Cisco c=IN Subject: Name: Root-CA cn=Root-CA ou=TAC o=Cisco c=IN Validity Date: start date: 16:17:31 UTC Oct 8 2013 end date: 16:57:31 UTC Oct 8 2013 Associated Trustpoints: cvo-pki Certificate Certificate Serial Number (hex): 08 <snip> Subject: Name: DMVPN-HUB1-NEW.cvo.IN.Cisco.Cisco Validity Date: start date: 15:57:05 UTC Oct 8 2013 end date: 16:17:31 UTC Oct 8 2013 Associated Trustpoints: cvo-pki !--- This is the old/expired ID cert. CA Certificate Status: Available Certificate Serial Number (hex): 05 <snip> Subject: Name: Root-CA : Validity Date: start date: 15:37:31 UTC Oct 8 2013 end date: 16:17:31 UTC Oct 8 2013 Associated Trustpoints: cvo-pki !---` This is the old/expired CA cert.

- CSCuj80062

  Symptom: Unexpected RP reload in asr1k.

  Conditions: Stream of corrupted ATM cells on idle VCC due to SIP hardware failure.

  Workaround: There is no workaround.

- CSCuj84219

  Symptom: Error messages shown on KS after SW upgrade to 15.2(4)M. Whenever a GM with multiple GDOI groups registers, an error message is logged on the respective KS: Oct 4 11:31:28.477 CEST: %CRYPTO-6-IKMP_NO_ID_CERT_FQDN_MATCH: ID of ce-de-xxxxx.wan.domain.net (type 2) and certificate fqdn with ce-de-xxxxx

  Conditions: Multiple GDOI groups with different GETVPN local-addresses configured on GM. GM/KS are ISR G2 routers running on 15.2(4)M code.

  Workaround: Configure "crypto isakmp identity dn", i.e. set the ISAKMP identity to the distinguished name (DN) of the router certificate. http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c4.html#wp1060149

- CSCuj85993

  Symptom: A Cisco ASR1006 (RP2) running Cisco IOS-XE Version: 03.07.04.S (asr1000rp2-adventerprisek9.03.07.04.S.152-4.S4) will crash after a recent High Availability (HA) fail-over event.

Conditions: High Availability (HA) fail-over is implemented with RP2 on the Cisco ASR. When a fail-over is initiated to the active RP2 module (for example by removing the active RP2 module), the ASR fails over fine, but once a hold resume is initiated on an existing call (that was preserved from the fail-over), the ASR reboots.

Workaround: The crash is not observed on IOS-XE version 03.07.03.S

- CSCuj86393

  Symptom: cpp_cp process crashes on ESP100, ESP100 or ASR1002X.

  Conditions: Bring up 4k PPPoLNS sessions. Tear-down large number of sessions (eg. >3k) by performing "shut" on individual Dialer interfaces one-by-one on CPE.

  Workaround: There is no workaround

- CSCuj91680

  Symptom: ESP crashes running 3.9.1 when NAT enabled.

  Conditions: NAT must be enabled.

  Workaround: No known workaround .

  This change adds code to prevent a very rare crash that can occur when feature code does not complete a memory access correctly. The crashes are unreproducible.

- CSCuj96123

  Symptom: ASR1000 crashed with following log in crashinfo file: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SBC main process

  Conditions: the ASR1000 router is the standby router in CUBE-SP setup.

  Workaround: There is no workaround.

- CSCuj96893

  Symptom: Cisco router hangs and it stopped passing the traffic. Customer needs to reload the router to make it work until it hangs next time. It hangs sometimes once in month.

  Conditions: This issue is seen with more than one router.

  Workaround: There is no workaround.

  Symptom: Router hangs and it stopped passing the traffic. Customer needs to reload the router to make it work until it hangs next time. It hangs sometimes once in month.

  Conditions: issue is seen with more than 1 router.

  Workaround: There is no workaround.

- CSCul02786

  Symptom: The original issue fails silently and it is only detected via traffic or inspecting the hierarchy via the CLI, show plat hard qfp act feat qos que out int <ifname> hier detail. The QoS rates are in accurate due to a bad hierarchy. Subsequent crashes and the issue that is documented in this DDTS were regression from the original fix intended to build the hierarchy on ESP-100 correctly. All issues involved fair-queue in a flat or hierarchical policy when applied on the fly.

  Conditions: Applying fair-queue on the fly resulted in the bad hierarchy. As a result the provisioned services could not be guaranteed.

  Workaround: There is no workaround.

- CSCul04033

  Symptom: LDP stays down over Multilink when connecting to Juniper router

Conditions: Issue notice with latest IOS as same setup was working with 15.0(1)S1(3.1S) and earlier release.

Workaround: There is no workaround.

- CSCul04434

  Symptom: Given a GETVPN GM that is configured with an ipv6 crypto map, if that crypto map is applied to two interfaces (one common identity, e.g. loopback) and if certain configuration operations are performed, the GM will loose connectivity to the ipv6 group. If the GM has dual-stack interfaces with both an ipv4 and an ipv6 crypto map. The IPv4 GETVPN functionality will not be affected while triggering the event documented in this defect.

  Conditions: Performing configuration operations that follow the patterns described below : 0. IPv6 Crypto Map applied to two interface (E0/0 and E2/0, lets call them Primary and Secondary) At this stage all works well IPv6 traffic is encrypted between two test GMs. 1. Shut down Secondary interface (E2/0) Result, no change in functionality GM can still exchange encrypted IPv6 traffic with peers. 2. Remove the ipv6 crypto map from the Primary interface (E0/0, while E2/0 is in admin shutdown state). Result, IPv6 traffic is sent out in clear text 3. Re-apply crypto map to the Primary interface (i.e. E0/0) Result, no change, packets are still being sent out in clear text, even though GDOI sees the E0/0 interface as associated with the cry map and group. 4. Remove the crypto map from the Secondary interface which is still in shutdown state Result : No change in the behavior 5. Remove and re-apply the crypto map on the Primary interface Result : GM re-registers

  Workaround: Remove the ipv6 crypto map from the Secondary Interface before shutting it down.

- CSCul06361

  Symptom: When subscriber session is created with 'ip subscriber interface' on subinterface in shutdown state, after bringing the subinterface up, the 'out' pkt counters are not increasing. Subscriber does not have IP connectivity, since traffic is going only in one direction.

  Conditions: ASR1k ISG running IOS XE 3.7.4.S (15.2(4).S4), with 'ip subscriber interface' created from subinterface in shutdown state.

  Workaround: Clearing subscriber session when subinterface is up/up will re-establish session with connectivity restored.

- CSCul08311

  Symptom: SIP ALG will drop NAT traffic.

  Conditions: In a case, FQDN instead of IP address is included in the "c=" line of SDP in the 200 OK response, and SIP ALG will drop this message

  Workaround: A workaround is to turn off SIP ALG if SIP server (VCS) can support NAT traversal by itself. Another way is to let VCS fill IP address instead of FQDN in the "c=" line of SDP if possible.

- CSCul10907

  Symptom: ASR1002x or ASR1000 with an ESP100 may crash when Broadband MLPPP sessions with QoS applied are brought up or the sessions flap.

  Conditions: This issues causes a ASR1K crash (cpp_cp_svr) when a Broadband MLPPP bundle with QoS is applied is brought up or the session flaps. Problem is most prevalent on MLPPP Bundles with two or more member links. Affects MLPPPoE, MLPPPoA, MLPPPoEoA, and MLPPPoLNS.

  Workaround: There is no workaround

  This issue is only applicable to IOS 15.3(3)S1 / IOS-XE 3.10.1S.

- CSCul13619

Symptom: When incoming ESP packet has as final destination a local interface on the GM itself (including loopback), the packet is recirculated after decryption causing it to be dropped. If the decrypted packet is only a transit one, e.g. its for a host on a connected LAN, all works as expected.

Conditions: getvpn, ipv6 and use of ingress ipv6 access lists

Workaround: There is no workaround.

Symptom: When incoming ESP packet has as final destination a local interface on the GM itself (including loopback), the packet is recirculated after decryption causing it to be dropped. If the decrypted packet is only a transit one, for example, it is for a host on a connected LAN, all works as expected.

Conditions: This issue occurs due to getvpn, ipv6 and use of ingress ipv6 access lists.

Workaround: There is no workaround.

- CSCul16541

  Symptom: cpp_cp_svr crash with model F QoS and multiple PPPoEoA/PPPoA VCs on one or more ATM PVPs.

  Conditions: While bringing up multiple PPPoEoA/PPPoA sessions with model F QoS on one or more ATM PVPs.

  Workaround: There is no workaround

- CSCul27444

  Symptom: The as1002-x crashes while processing the MLPoLNS configuration. The model F configuration that would cause the crash is attached to the DDTS.

  Conditions: When a grandparent policy is attached to a vlan sub-interface configured as a queue, it needs to be converted to a leaf node schedule when a session (MLPPP member link) is added to the vlan. During the transformation of a queue to a leaf schedule, all queues were not moved in the same event as required due to a hardware restriction.

  Workaround: There is no workaround.

- CSCul31100

  Symptom: COS markings not seen Proper on the dot1q interface.

  Conditions: The issue will be seen if met any of following conditions: 1, Crypto-Map implemented in Transport mode implemented on Tunnel. 2, Fragment happened in data plane on the dot1q interface.

  Workaround: 1.Remove Encryption from the Tunnel or downgrade IOS to 15.0(1)S3 if the issue is happened with IPSec but no fragment; 2, No workaround if the issue occurs on a large packet (need fragment);

- CSCul31192

  Symptom: ESP may crash @ipv4_nat_alg_prune_sd

  Conditions: Seen with SIP traffic.

  Workaround: There is no workaround.

- CSCul39211

  Symptom: With an IOS router set as an EZVPN client, with either interactive (CLI) or HTTP-Intercept authentication enabled, if the user does not enter in proper credentials within 10 seconds, the router will resend AM3 to the EzVPN server. This causes a retransmission storm to trigger and quickly tear down the tunnel, which causes the authentication to fail.

  Conditions: IOS router acting as EzVPN client.

Workaround: 1) Have users enter credentials within 10 seconds of login prompt. 2) Save credentials on router so users don't need to enter them every time. 3) Downgrade to 15.1(4)M5 or earlier

- CSCul40500

  Symptom: MD5 is used to sign the PKCS10 embedded in SCEP encrypted message whatever hashing algorithm is configured under the relevant trustpoint or whatever the best hashing algorithm reported by the SCEP GetCACaps message is.

  Conditions: Using SCEP for router enrollment.

  Workaround: There is no workaround.

- CSCul48822

  Symptom: While provisioning an ISG IP Subscriber session it is possible to leak an ESS segment chunk (IOSXE ESS SEG).

  Conditions: The memory leak may occur when there is an error provisioning an ISG IP subscriber session.

  Workaround: There is no workaround.

- CSCul48865

  Symptom: Some static vrf NAT entries which are stored in the startup-config don't appear in the show running.

  Conditions: After reloading the router.

  Workaround: There is no workaround. Once hitting the symptom, reconfigure those NAT entries.

  Those nat entries are actually appear in the nat translation table

- CSCul50570

  Symptom: A hardware interrupt causes service outage and a micro-code core will be generated. This condition puts the router in an inoperable state. This issue would affect bundle interfaces such as MLPPP and GEC aggregate mode.

  Conditions: While processing dynamic reconfiguration events, one of the scheduling node is left in a committed but not forward state. When a flush packet is injected in a flush queue to complete the reconfiguration process, it causes a hardware interrupt when it traverses the node that was left in a non-forwarding state.

  Workaround: There is no work around.

- CSCul54111

  Symptom: This issue causes the ESP to crash while applying QoS Model F. The issue occurs with both small and scaling configuration. The problem occurs all ESPs including ISR and CSRs.

  Conditions: The problem occurs with both small and large configurations. It is timing related as it occurs after running asynchronously in which case the code executes the deferral path which was not clear the event processing flags upon completion. When these flags are not cleared, the code treats the condition as fatal; hence the ESP crash. While Model F is understood to be impacted by this problem it is conceivable this issue could occur with any configuration where the target interface handle for the policy is different from the parent interface handle, e.g. vlan queue on a GE interface. Model F Sample Configuration: policy-map grandparent class class-default shape average 10000000 class-map match-all p0 match precedence 0 class-map match-all p1 match precedence 1 class-map match-all p2 match precedence 2 policy-map child class p0 priority police cir 2000000 class p1 bandwidth remaining ratio 10 class class-default bandwidth remaining ratio 1 policy-map parent class class-default shape average 10000000 bandwidth remaining ratio 1

service-policy child interface GigabitEthernet0/0/0.4 encapsulation dot1Q 2 service-policy output grandparent The parent policy would typically be applied on a session on the vlan. The issue would typicall occur when the grandparent policy is processed on ESP.

Workaround: There is no workaround for this issue.

- CSCul55038

  Symptom: In mpls-vpn scenario, when the size of packet coming from core network is bigger than mtu set on CE facing interface, the expected ICMPv6 TOO_BIG fail to return.

  Conditions: 1. packet is bigger than mtu on CE facing interface. 2. the packet come from core mpls network and try to go through CE facing interface. 3. the issue is found on PE in mpls-vpn scenario.

  Workaround: Enable IPv6 on core facing interface, which is receiving the mpls packet to CE.

- CSCul64097

  Symptom: ZBFW SYN cookie counter shows positive number although the real number of half open sessions have dropped to zero. Since the counter is used to trigger SYN cookie once it is over the configured limit, this is causing the SYN cookie protection to always kick in regardless of the real situation, which drags down the network performance.

  Conditions: SYN cookie feature needs to be configured, and it is configured to protect per VRF or global number of half open sessions. The counter error only happens under some race condition which needs particular and supposedly high traffic load to trigger.

  Workaround: Disable the SYN cookie.

  The counter problem only happens under certain corner case. When the counter goes wrong, the SYN cookie protection logic could be triggered erroneously.

- CSCul64664

  Symptom: After VC goes down, that packets are received on xconnect interface are leaked.

  Conditions: -when VC goes down -Unicast packet with TTL>=2 are received on that xconnect interface -When having the route for the destination of the unicast packets

  Workaround: -remove the route from the routing table -apply an ACL to deny these leaked packets

- CSCul66644

  Symptom: IP/PPPoE stack terminated on QinQ subinterface is not working as soon as interface has been removed and created back with adjusted configuration

  Conditions: - QinQ subinterface configured with second-dot1q VLAN IDs range - Interface removed and created back

  Workaround: - Remove affected subinterface - Create a new one with another ID

  Problem is most likely seen when creating and deleting the same interface within a short period of time, as might be done by applying a configuration script.

- CSCul67310

  Symptom: ASR1K microde crash with either of the following errors
  SOR_CSR32_SOR_ERR_LEAF_INT__INT_SOR_OPF_GRANT_PTCL_UVF
  OPF_CSR32_OPF_LOGIC_ERR_LEAF_INT__INT_START_OF_BURST_MARKER_ERR

  Conditions: This issue ONLY affects on ASR1002x and ASR1K RP2/ESP100 based platforms running 15.2(4)S, 15.3(1)S, 15.3(2)S, 15.3(3)S, and 15.4(1)S based images. This issue can occur on platforms with scaled sub-interface or broadband session configurations when the number of sub-interfaces or sessions on a interface is reduced from > 4000 to less than 4000 and moderate to heavy traffic flow is occurring at the time that the sub-interface or session count is reduced. If the the ASR1K is operating below this threshold or above this threshold this issue is not seen.

Workaround: There is no workaround. This issue is a result of a scheduling hierarchy restructuring issue when the number of sessions is reduce such that we drop below this 4000 sub-interface or broadband session threshold on a interface. As indicated above, if the sub-interface or broadband session count is below 4000 or consistently above 4000 this issue should not be seen.

- CSCul78163

  Symptom: cpp_cp_svr process crashes.

  Conditions: On ESP100, ESP200 or ASR1002X platforms, when scaling over 4000 nodes on an interface or sub-interface and then nodes are removed or deleted so the total drops below 4000, the cpp_cp process can crash. This can also happen on all ASR1K platforms with ATM interfaces when moving ATM VCs from one COS to another COS and then deleting the ATM VCs at the same time.

  Workaround: Avoid scaling past 4000 scheduling nodes on the same interface or sub-interface on ESP100, ESP200 or ASR1002X when there is a chance the nodes can come and go causing the total to drop below 4000. Avoid deleting ATM VCs at the same time the VC is being reconfigure with a different COS value.

- CSCul81725

  Symptom: cpp_cp_svr on ESP crashes.

  Conditions: When configuring MLPoEoPTA, the control plane events generated to the data plane cause the data plane to crash if the events are generated in a certain order. This is highly dependent upon timing between the control plane and data plane.

  Workaround: There is no workaround.

- CSCul93292

  Symptom: Ucode crash with alg traffic when there are flow passing through pysical interface with nat configuration vasi interface with nat configuration in the same box

  Conditions: Ucode crash with alg traffic

  Workaround: disable all the algs

- CSCul93523

  Symptom: CPP 0 failure Stuck Thread(s) detected

  Conditions: Setting up about 2.2kps traffic with both nat/non-nat packets.

  Workaround: There is no workaround

- CSCul94622

  Symptom: On an ASR router with ct3 SPA, Malloc Failures and SPA F/W download failures are seen.

  Conditions: SPA should have many channels configured (> 50 % of its max capacity) and SPA soft reload is done

  Workaround: There is no workaround

- CSCum09702

  Symptom: OSPF neighbours can not establish FULL adjacency over dmvPN tunnels

  Conditions: dmVPN with OSPF is configured on IOS-XE platforms

  Workaround: there is no workaround

1.DMVPN can't support adjid=0 & maybeL2 now.Cause related func(mcprp_inject_fill_macstring_pak_encap) only for (TUN_MODE_GRE_IP & TUN_MODE_IP_IP). It will not modify tunnel code this time. 2.For this ticket, we will fix it in ospf perspective.In mcprp_inject_check_type, add ospf special if condition, if it is incomplete, will return failed.The first pkt will drop.Ios trigger arp,then send related ospf unicast pkt.

- CSCum12911

  Symptom: Issue a 'write mem' before the next renewal timer is triggered. The renewal fails with: %PKI-6-CERTRENEWMANUAL: Please renew the router certificate for trustpoint xxxx

  Conditions: IOS is configured as SCEP client, with an auto-enroll timer. Also, instead of 'enrollment url' under the trustpoint, an enrollment profile is configured. 'show crypto pki timers' should show a renew timer as per the configuration.

  Workaround: Use 'enrollment url ..' directly under the trustpoint.

- CSCum13126

  Symptom: After initiating an RP fail-over either through redundancy force-switchover or by using test crash, MLPPP interface remains down though T1's are up. Either shut/no shut of 1 of the member links or clear ppp all brings the MLPPP interface back up.

  Conditions: Trigger : RP fail-over seems to be the Trigger, apart from which there do not have to be any associated config changes made.

  Workaround: unknown

- CSCum22612

  Symptom: Since the ASR fails to send MM6 [being a responder] in the absence of a valid certificate, IKE SAs start leaking and hence get stuck in MM_KEY_EXCH state. Multiple MM_KEY_EXCH exist for a single Peer on the ASR, however the Peer does not retain any SAs for ASR in this case. Along with CAC for in-negotiation IKE SAs, these stuck SAs block any new SAs or IKE rekeys even after renewing the certificates on the ASR.

  Conditions: - ASR acting as IKEv1 termination point [sVTI for example] and is a responder. - IKE authentication mode is RSA-SIG [Certificates]. - On the ASR, the ID-Certificate is either Expired or Not-present for a given sVTI tunnel - The ASR also has a IKE in-negotiation CAC of a certain value. Example: crypto call admission limit ike in-negotiation-sa 30

  Workaround: a) Manually delete stuck SAs by using: clear crypto isakmp 12345 .. where 12345 is conn_id of a stuck SA. Repeat this for each stuck SA b) Temporarily increase CAC to accommodate new SA requests: crypto call admission limit ike in-negotiation-sa 60

  Found and Tested in XE 3.7.4 [15.2(4)S4]

- CSCum43217

  Symptom: Continuous reloads of an ASR running IOS XE with core files being generated on the router.

  Conditions: ASR running IOS XE with SIP ALG enabled and SIP traffic being translated via NAT.

  Workaround: Remove SIP ALG translations under NAT using the command: no ip nat service sip tcp

- CSCum94408

  Symptom: Intermittently, if the situation is such that Root's CRL to validate Sub does not get downloaded [Internal or External failures], whereas the CRL by Sub gets downloaded, we will see: [Debug crypto isakmp and Debug crypto pki m/t/v/c] ISAKMP (35845): adding peer's pubkey to cache ISAKMP:(35845): processing SIG payload. message ID = 0 %CRYPTO-3-IKMP_QUERY_KEY: Querying key pair failed.

Conditions: IOS configured with the IKEv1, Authentication mode RSA-SIG [Certificates]. PKI Infrastructure is as follows: Root -> Sub -> ID - Root and Sub Trustpoint Have "revocation-check crl none" - Sub has "chain-validation continue Root"

Workaround: Disable Revocation-check and Chain-validation under Sub Trustpoint.

Enable isakmp diagnostics: crypto isakmp diag error 50 Once the sessions fail: show crypto isakmp diag error count - Should show "Failed to find public Key" and show crypto isakmp diag error - Should show tracebacks under: failed to find public key

- CSCum96156

  Symptom: IOS will fail to match the certificate map intermittently

  Conditions: IOS PKI using certificate maps, to authorize the Peer certificates or override CDP. In this case: - if a certificate map is written on a PC, with upper case letters in them: Ex: crypto pki certificate map HR-Users 10 subject-name co ou = HR-Users - and this is a part of the configuration that is merged with the running config through IOS file-system [directly from flash or FTP/TFTP/HTTP etc], IOS retains the upper case letters. [contrary to certificate maps written through CLI, always converts everything to lower case letters]

  Workaround: A) - copy the certificate maps [that have upper case letters in them] to a notepad - remove the certificate maps [that have upper case letters in them] - paste the certificate maps, through IOS CLI - wherever these cert maps were being called, they will stay intact, and this change will take effect immediately or B) - The certificate map needs to enter IOS in a manner that IOS would insert it if you were to enter it in a CLI I.e. Make sure the external config generators generate the certificate map in such a way that everything is in lower case, and it has white spaces between DN OID, '=' and the value.

- CSCum98137

  Symptom: FP reloads due to cpp_cp process crash.

  Conditions: Creating a session w/QOS policy and applying a shaper on VLAN for the session where both of these events occuring at the same time.

  Workaround: There is no workaround

- CSCun02711

  Symptom: observing cpp_cp_svr crash

  Conditions: Interface Flap with Model4 QoS under Oversubscribe load

  Workaround: There is no workaround

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.4aS

This chapter contains the following section:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.4aS

This section documents resolved issues on Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.4aS.

- CSCuj45418

  Symptom: ASR1002-X reloads with the corefile reporting `CIF_CSR32_CIF_CIF_MISC_GRP2_ERR_LEAF_INT__INT_CIF_EPIFC_CRC_ERR interrupt.`

  Conditions: This condition is applicable only to ASR1002-X running IOS images prior to IOS XE3.7.4aS. The issue is not specific to any configuration or traffic pattern.

  Workaround: There is no workaround. The issue is fixed in IOS XE3.7.4aS and later releases.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.4S

This chapter contains the following sections:

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.4S

This section documents the unexpected behavior that might be seen in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.4S.

- CSCui22356

  Symptom: The Subpackage ISSU Upgrade is performed on ASR1002-X router after upgrading the standby RP (R0/1) with new RP subpackages. Then, Switchover is forced from the active IOS process to the standby IOS process. During the switchover, new active RP performs configuration Bulk-Sync with the standby RP. During this Bulk Sync operation, the configuration related to the interfaces is not synchronized with the standby RP due to Bulk Sync MCL failures. The following error message will be displayed when this error is present.

  Sample Error Message:

```
<.............>
Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check full
list of mismatched commands via:
  show redundancy config-sync failures mcl
Config Sync: Starting lines from MCL file:
interface Tunnel150
 ! <submode> "interface"
- tunnel source GigabitEthernet0/0/0.34
<..............>
Standby takes more time(~744 seconds) for reaching terminal State.
```

  Conditions: The symptom is observed after redundancy force-switchover step in ISSU upgrade procedure.

Workaround: Peform a standby IOS reload using the following command:

hw-module subslot R0/0 reload

- CSCtx72973

  Symptom: Config-sync failiure is seen when unconfiguring the crypto gdoi group.

  Conditions: Seen on HA setup.

  Workaround: There is no workaround.

- CSCtz49200

  Symptom: OSPF IPv6 control packets are not encrypted or decrypted.

  Conditions: This issue occurs while configuring the IPv6 OSPF authentication.

  Workaround: There is no workaround.

- CSCua90097

  Symptom: flexVPN client ikev2 sa stuck at IN-NEG with status description: `Initiator waiting for AUTH response.`

  Conditions: flexVPN server initial **clear crypto session** command to clear 4K crypto sessions. After crypto session recovered, there is 1 ikev2 sa at flexVPN client stuck at IN-NEG status. At flexVPN server, there is no ikev2 peer, 172.4.234.1.

  ```
  Client: 2ru-2#sh crypto ikev2 sa local 172.4.234.1 det
  Load for five secs: 12%/1%; one minute: 9%; five minutes: 9%
  Time source is NTP, 11:49:38.299 PDT Thu Jul 5 2012
  Tunnel-id Local         Remote              fvrf/ivrf    Status   1
  172.4.234.1/500       172.255.255.252/500   none/none    IN-NEG
  Encr: AES-CBC,   keysize: 256,   Hash: SHA512,  DH Grp:5,    Auth sign: PSK, Auth
  verify: Unknown - 0    Life/Active Time: 86400/0 sec      CE id: 50798, Session-id: 0
  Status Description: Initiator waiting for AUTH response
  Local spi: 7E92CB576E3BC65B       Remote spi: 01B87002CE230A4A
  Local id: 2ru-2-1000.cisco.com       Remote id:        Local req msg id:  1
  Remote req msg id:  0                 Local next msg id: 2
  Remote next msg id: 0                 Local req queued:  1
  Remote req queued:  0                 Local window:      5
  Remote window:   1             DPD configured for 0 seconds, retry 0
  NAT-T is not detected          Cisco Trust Security SGT is disabled        Initiator
  of SA : Yes     2ru-2#
  ```

  Workaround: flexVPN client is able to use the **clear crypto ikev2 sa psh <index>** command to delete stuck ikev2 sa.

- CSCuh20209

  Symptom: ucode crashes when running the **clear ip nat translations** command.

  Conditions: This condition occurs very rarely with stateful traffic.

  Workaround: Use **clear ip nat translations vrf** *vrf_name* command to clear VRF aware translations.

- CSCuh87017

  Symptom: Hw-Sw: ASR1004 ASR1000-RP2 ASR1000-ESP20 asr1000rp2-adventerprisek9.03.09.01.S.153-2.S1. The ESP goes down logging messages as shown below:

  ```
  Jun 27 19:59:12.308: %CPPHA-3-FAULT: F0: cpp_ha:  CPP:0.0 desc:CPP Client process
  failed: cpp_cp det:HA class:CLIENT_SW sev:FATAL id:1 cppstate:RUNNING res:UNKNOWN
  flags:0x0 cdmflags:0x0  Jun 27 19:59:12.393: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_ha:
  ```

```
cpp_ha encountered an error    -Traceback= 1#e1875e79d5b29fc4e498ecbc61cdf452
errmsg:F6DB000 2230 cpp_common_os:FF5A000 C330 cpp_common_os:FF5A000 C130 :10000000
6FA4 :10000000 12718 evlib:F435000 E3B8 evlib:F435000 10564 cpp_common_os:FF5A000
12FF8 :10000000 F108 c:E51F000 1E938 c:E51F000 1EAE0  Jun 27 19:59:13.054: %PMAN-3-
PROCHOLDDOWN: F0: pman.sh:  The process cpp_cp_svr has been helddown (rc 134)  Jun 27
19:59:14.289: %PMAN-0-PROCFAILCRIT: F0: pvp.sh:  A critical process cpp_cp_svr has
failed (rc 134)  Jun 27 19:59:18.422: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_ha:  cpp_ha
encountered an error -Traceback= 1#e1875e79d5b29fc4e498ecbc61cdf452   errmsg:F6DB000
2230 cpp_common_os:FF5A000 C330 cpp_common_os:FF5A000 C130 :10000000 6FA4 :10000000
12718 evlib:F435000 E3B8 evlib:F435000 10564 cpp_common_os:FF5A000 12FF8 :10000000
F108 c:E51F000 1E938 c:E51F000 1EAE0
```

Conditions: On issuing **show ip nat trans** command when there are a large number of static networks translations the ESP may reset with the above messages. The issue is caused by a calculation dealing with the number of static network translations that are configured. It is possible to avoid this issue by moving out of the impacted range of static network translations.

Workaround: Determine the number of static network translations:

```
Router# show platform hardware qfp active feature nat datapath stats | include static
net         non_extended XXXX entry_timeouts XXXX statics XXXX static net 126 hits
XXXX misses XXXX    Take the number of static network translations ("static net") and
divide it by 32, and then look at the remainder:    126/32 = 3 remainder 30    If the
remainder is 30 or 31 this issue could be encountered when the 'show ip nat
translation' is executed.  To avoid this situation add or remove one or two static
network translations, for example:    ip nat inside source static network X.X.X.X
Y.Y.Y.Y /ZZ  ip nat inside source static network A.A.A.A B.B.B.B /CC    The addresses
used in these two static network translations do not need to be hit by any traffic,
and do not need to be subnets that are regularly used within the network.  Next verify
that the remainder is no longer 30 or 31:    Router#$show platform hardware qfp active
feature nat datapath stats | include static net         non_extended XXXX
entry_timeouts XXXX statics XXXX static net 128 hits XXXX misses XXXX    128/32 = 4
remainder 0    This can also be accomplished by removing one or two static network
translations to lower the remainder.  More Info: Symptom: Hw-Sw:   ASR1004  ASR1000-
RP2  ASR1000-ESP20   asr1000rp2-adventerprisek9.03.09.01.S.153-2.S1  The ESP goes down
logging messages similar to what is shown below: Jun 27 19:59:12.308: %CPPHA-3-FAULT:
F0: cpp_ha:  CPP:0.0 desc:CPP Client process failed: cpp_cp det:HA class:CLIENT_SW
sev:FATAL id:1 cppstate:RUNNING res:UNKNOWN flags:0x0 cdmflags:0x0 Jun 27
19:59:12.393: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_ha:  cpp_ha encountered an error   -
Traceback= 1#e1875e79d5b29fc4e498ecbc61cdf452   errmsg:F6DB000 2230
cpp_common_os:FF5A000 C330 cpp_common_os:FF5A000 C130 :10000000 6FA4 :10000000 12718
evlib:F435000 E3B8 evlib:F435000 10564 cpp_common_os:FF5A000 12FF8 :10000000 F108
c:E51F000 1E938 c:E51F000 1EAE0 Jun 27 19:59:13.054: %PMAN-3-PROCHOLDDOWN: F0:
pman.sh:  The process cpp_cp_svr has been helddown (rc 134) Jun 27 19:59:14.289:
%PMAN-0-PROCFAILCRIT: F0: pvp.sh:  A critical process cpp_cp_svr has failed (rc 134)
Jun 27 19:59:18.422: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_ha:  cpp_ha encountered an
error -Traceback= 1#e1875e79d5b29fc4e498ecbc61cdf452   errmsg:F6DB000 2230
cpp_common_os:FF5A000 C330 cpp_common_os:FF5A000 C130 :10000000 6FA4 :10000000 12718
evlib:F435000 E3B8 evlib:F435000 10564 cpp_common_os:FF5A000 12FF8 :10000000 F108
c:E51F000 1E938 c:E51F000 1EAE0
```

- CSCuh90658

  Symptom: QFP crash.

  Conditions: This symptom occurs under the following conditions:

  - Create normal GTPv1 session and primary PDP.
  - Delete request with teardown false.
  - Update QoS with different data TEID at both SGSN and GGSN when crash occurred.

  Workaround: There is no workaround.

- CSCui07002

Symptom: When two routers attempt to build an IKE session and use PKI for authentication, if the CRL has expired, the responding router crashes and reloads.

Conditions: PKI chain-validation, CRL check, expired CRL

Workaround: Disable CRL check.

- CSCui38300

  Symptom: High latency is observed in customer network.

  Conditions: Under conditions such as forced test, it is possible to create scenarios where flow-lock contention is very high because of NAT gatekeeper failures.

  Workaround: There is no workaround.

- CSCui40812

  Symptom: CUBE responds with 491 for RE-Invite with a=recvonly during HOLD.

  Conditions: ++ SIP RE-Invite to deactivate the media with (c=IN IP4 0.0.0.0 and a=recvonly) is causing CUBE to respond with 491 on IOS "asr1001-universalk9.03.06.02 .S.152-2.S2" where as on IOS "asr1001-universalk9.03.04.01 .S.151-3.S1" CUBE is responding with 200 ok with a=inactive.

  Workaround: There is no workaround.

- CSCui61103

  Symptom: DMVPN Phase 3 NHRP refresh clears RIB/NHO flag and RIB is not updated.

  Conditions: When an NHRP Phase 3 child mapping entry is refreshed the mapping entry loses its 'rib' and 'nho' flags and the corresponding RIP route is either removed (rib) or the next-hop-override is removed (rib + nho).

  Workaround: There is no workaround.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.4S

This section documents resolved issues on Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.4S.

- CSCtj24692

  Symptom: NVRAM configuration file gets corrupted when a chassis is power cycled without a graceful shutdown.

  Conditions: Power cycle an ASR chassis without graceful shutdown.

  Workaround: Shutdown chassis using the **reload** command and make sure RP gets to ROMMON before power cycling the chassis.

- CSCtj61284

  Symptom: NAT overload does not work for non-directly connected destinations in MPLS-VPN configurations.

  Conditions: The symptom is observed with NAT overload configured to NAT traffic coming over an MPLS VPN to internet via a VRF-enabled interface.

  Workaround: There is no workaround.

- CSCtj96278

Symptom: T38 fax relay call speed is set to 14.4k regardless of the "fax rate" CLI configuration.

Conditions: There is no condition.

Workaround: There is no workaround.

- CSCtl55445

  Symptom: CUBE logs the following message: `%SIP-3-INTERNAL: Cannot insert call history entry for callID.`

  Conditions: Calling party cancels call before connection. The following is an example:

```
INVITE     --------------->---------------->    100 Trying     <---------------<------
----------    180 Ringing     <---------------<----------------    CANCEL     -------
--------->---------------->    200 OK     <-----------------<-----------------    487
Request Cancelled     <-------------------<---------------       ACK
```

  Workaround: There is no workaround.

- CSCto81601

  Symptom: If there is a problem with publishing the CRL, a major problem must exist so that further publishing is suspended until the issue is addressed, and the CA requires a shut or no shut. Currently there is no error message which suggests what happened with CRL. Need to add proper error messaging to make it more interactive.

  Conditions: There is no condition.

  Workaround: Enter "shut" or "no shut" on the CA server should result in the CRL being published again.

- CSCtr88785

  Symptom: When following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.

  Conditions: This symptom is observed on a Cisco 3845 running the c3845-advipservicesk9-mz.151-4.M1 image with a PKI certificate server configuration..

  Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCts34256

  Symptom: We send 1M prefixes to an ASR with 8G of memory. The memory status is seen as critical. However this stays as critical even days after the BGP peering is removed. The fman_rp process seems to be holding the most memory even when the BGP routes are cleared. The impact of this is unknown at this time.

  Conditions: This symptom is observed on a Cisco 3845 running the c3845-advipservicesk9-mz.151-4.M1 image with a PKI certificate server configuration..

  Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtt45299

  Symptom: Failed to join the Meetme conference.

  Conditions: If there's person already join the conference.

  Workaround: There is no workaround.

- CSCtx99353

  Symptom: The following error message appears: `%SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level.`
  This error message can lead the device to crash.

  Conditions: Seen on HA setup.

Workaround: Remove the route list from Multicast MOH CLI so that Cu can still have music on hold and can continue the feature. Alternatively, disable MOH (no Music comes on hold).

- CSCty26035

  Symptom:

  - There is a discrepancy in the inbound and the outbound SA lifetime in thestandby router.
  - The KB lifetime in a standby router is greater than that of the active router, when a KB lifetime rekey occurs.
  - The ping will not go through after applying a dynamic crypto map.

  Conditions: The issues are seen after establishing the session between the HA routers and various test conditions.

  Workaround: There is no workaround.

- CSCty31407

  Symptom: netsync configuration for E1 (option 1) does not working.

  Conditions: Configure R0 as netsync source, the netsync source doesnt lock (only option 1) , option 2 works fine.

  Workaround: There is no workaround.

- 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.

- CSCty91566

  Symptoms: Potential memory leak is seen when handling DNS lookup response.

  Conditions: This symptom occurs when handling DNS lookup response.

  Workaround: There is no workaround.

- CSCtz58718

  Symptoms: CEF switching is not working with GRE + protected tunnel configuration.

  Conditions: Packets should go through tunnel interface.

  Workaround: There is no workaround.

- CSCtz96750

  Symptoms: Expected SPI is not populated after Authentication is configured.

  Conditions: Issue is seen for IPV6.

  Workaround: The problem is seen only in case of VL configuration.

- CSCua26931

  Symptoms: Calls placed on hold by 3rd Party SIP Server are disconnected if media inactivity is configured.

Conditions: PRI -- GW -- SIP -- 3rd Party SIP Server. Media inactivity is configured on the SIP GW. Phone behind the call server puts the call on hold. If the 3rd Party SIP server uses RFC 3261 hold (a=inactive) the call drops. If the 3rd Party SIP server uses RFC 2543 hold (c=0.0.0.0 and a=sendonly).

Workaround: Set media inactivity timer to a large value.

- CSCua35161

  Symptoms: On DMVPN HUB, some crypto maps still exist after removing Tunnel protection from tunnel interface.

  Conditions: It happens with scaling test.

  Workaround: There is no workaround.

- CSCua36330

  Symptom: Trace backs found.

  Conditions: While copying the text file from the certificate server. Accessing https://msca-root/test.txt.

  Workaround: There is no workaround.

- CSCua59513

  Symptom: Transform comp-lzs is not supported with current hardware configuration.

  Conditions: For ikev2_sanity script ,while testing the miscellaneous testcase Transform comp-lzs is not supported with current hardware configuration.

  Workaround: There is no workaround.

- CSCua62348

  Symptom: IKE TUNNEL HISTORY TABLE/ipsecGlobalValues/cipSecSpiStatus failed.

  Conditions: It should give correct data.

  Workaround: There is no workaround.

- CSCua65780

  Symptom: After a rollover, RA server does not retry to obtain its rollover CS cert from the CA server.

  Conditions: The issue is seen after the RA has rolled over once and its first enrollment request (post-rollover) sent to the CA server has failed for some reason.

  Workaround: There is no workaround.

- CSCua75781

  Symptom: CME reloads for E911 call ELIN translation for incoming FXS/FXO trunk.

  Conditions: The symptom is observed from Cisco IOS interim Release 15.3(0.2)T.

  Workaround: There is no workaround.

- CSCua78616

  Symptom: Not able to retrieve Via header for sending OPTIONS response back.

  Conditions: This issue is seen in OPTION message case.

  Workaround: Use the las_option_request from ccb while retreiving Via header.

- CSCua78771

  Symptom: Error message display needs cosmetic changes to follow style guide.

Conditions: In rare situation, we hit error message regarding an error situation. The message format needs to be updated to follow style guidelines.

Workaround: There is no workaround.

- CSCua80616

  Symptom: SPA handle invalid message is seen after running the **hw-module subslot** *x/y* **shut** command on ELC.

  Conditions: When multiple ELC sources are configured, such as primary and secondary network clock sources from ELC, and execute ELC shut using **hw-module subslot** *x/y* **shut** command, the SPA invalid handle error message is displayed.

  Workaround: There is no workaround.

- CSCua88511

  Symptom: Ipsec sas not setup correctly on uut1 = secp53-6.

  Conditions: Negative testcase failed because expect_ncomp is 77, ncomp is 78 , compf is 0(this particluar number should be 7), expect_compf is 8.

  Workaround: There is no workaround.

- CSCub01509

  Symptom: ESP reload on ASR1002-X and ISR4451.

  Conditions: Very High traffic rate of fragmented packets recieved with NAT configured(or traffic loop).

  Workaround: Eliminate unnecessary fragments using either: MTU tunning, ACL filter, diverting the packet to new interface without NAT.

- CSCub18622

  Symptom: Dynamic ACL does not get applied to the interface ACL, but the user shows up in the **show ip auth-proxy cache** command output.

  Conditions: Very High traffic rate of fragmented packets recieved with NAT configured(or traffic loop).

  Workaround: Move the auth-proxy rules onto a physical interface.

- CSCub34534

  Symptom: A basic call between 2 SIP phones over SIP trunk (KPML-enabled) fails.

  Conditions: This symptom is observed with Cisco ISR G2 platforms.

  Workaround: There is no workaround.

- CSCub46423

  Symptom: Connecting from Windows 7 L2TP/IPSec client to the VPN fails when using HSRP virtual IP as a gateway IP and Error 788 is displayed.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T or later releases, and the Windows 7 L2TP/IPsec VPN client.

  Workaround: Downgrade to Cisco IOS Release 15.1(3)T.

- CSCub52278

  Symptom: DVTI Virtual Access interface may flap during rekey with a large number of IKEv2/IPSec tunnels.

  Conditions: IKEv2 in large scale deployment is used.

Workaround: There is no workaround.

- CSCub79487

  Symptom: Traffic flow is not fine with Fragementation.

  Conditions: None.

  Workaround: There is no workaround.

- CSCub79543

  Symptom: CLI changes in the **show spi details** command

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

  Workaround: There is no workaround.

- CSCub84076

  Symptoms: CRYPTO MAP ACL FILTERING TEST FAILED due to indent counters.

  Conditions: CRYPTO MAP ACL FILTERING TEST FAILED due to indent counters.

  Workaround: There is no workaround.

- CSCub93641

  Symptoms:The load balancing feature of the flex-vpn solution of Cisco IOS does not provide authentication facilities to avoid non authorized member to join the load balancing cluster. Thus, an attacker may impact the integrity of the flex-vpn system by inserting a rogue cluster member and having the load balance master to forward VPN session to it. A number of secondary effect, including black-holing of some of the VPN traffic may be triggered by this issue.

  Conditions: Flex-VPN with Load Balancing feature active.

  Workaround: Using CoPP and interface access-list may be used to allow only trusted router to join the load balancer cluster PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3 or 3.9

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:W/RC:CCVE ID CVE-2012-5032 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

- CSCub97881

  Symptoms: Few Mem leak seen in HSRP-CLB notification in scaled IKEv2 load-balancing cluster scenario.

  Conditions: Scaled IKEv2 load-balancing cluster scenario. Crypto Load Balancer HSRP state change [Master->Slave] or [Slave->Master]. IOS TCP process cleaning up internal message which has pointer to meory which CLB has allocated.

  Workaround: There is no workaround.

- CSCuc01194

  Symptom: If there is a "peer .. fqdn ..." statement in the startup-config

  For example: crypto ikev2 client flexvpn flex peer 1 fqdn <FQDN>

  Then after rebooting, the "peer ..." statement may be missing from the running-config.

  Conditions: This occurs because at boot time, when the startup-config is parsed, there is no DNS connectivity so the DNS resolution of the FQDN fails and hence the command is not accepted.

Workaround: Remove the peer and add it again with the "dynamic" keyword, i.e.: crypto ikev2 client flexvpn flex no peer 1 fqdn <FQDN> peer 1 fqdn <FQDN> dynamic

Note This process will delay the DNS resolution of the fqdn until the VPN tunnel is built.

- CSCuc02931

  Symptoms: FlexVPN site to site crypto session at UP-NO-IKE status.

  Conditions: Clear cry session is given during rekey, create new sa with invalid spi, invalid SPI do not delete

  Workaround: Shut or no shut the tunnl interface.

- 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.

- CSCuc09667

  Symptoms: Router experiences crashes due to SIP due to a freed pointer in memory.

  Conditions: There is no conditions.

  Workaround: There is no workaround.

- CSCuc11809

  Symptoms: The number if IPSec SAs on the box keeps increasing.

  Conditions: IPSec eekeys are happening due to volume lifetime exhaustion.

  Workaround: Turn off volume based rekey.

- CSCuc22655

  Symptom: IOS Router Identity Certificate missing upon reboot.

  Condition: Identity certificate imported into a trustpoint that does not contain the direct issuer Certificate Authority certificate.

  Workaround: Import the identity certificate into the trustpoint which contains the issuer's certificate.

- CSCuc25995

  Symptom: A router unexpectedly reboots and a crashinfo file is generated. The crashinfo file contains an error similar to the following:

```
%ALIGN-1-FATAL: Illegal access to a low address 04:52:23 UTC Wed Sep 19 2012
addr=0x4, pc=0x26309630z , ra=0x26309614z , sp=0x3121BC58
```

  Condition: This occurs when IPsec is used. More precise conditions are not known at this time.

  Workaround: There is no workaround.

- CSCuc28138

  Symptom: Tracebacks are seen.

  Condition: When protocol mode dual-stack is enabled under telephony-service and create cnf-files is executed.

Workaround: There is no workaround.

- CSCuc29179

  Symptom: The Cisco ASR 1000 Series Aggregation Services Router filters out the ARP requests with its own source address. This leads to ping failure between two interfaces, which belong to different vrf and own same IP subnet; for example, vrf v1 1.0.0.1/24 and vrf v2 1.0.0.2/24.

  Conditions: The gigabit ethernet interface (gig0/0/0) connected b2b to another interface on same router with VRF configured on atleast one of the interfaces.

  Workaround: Configure some MAC address on the gigabit ethernet interface (gig0/0/0) and then unconfigure the MAC address.

- 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.

- CSCuc44749

  Symptom: Audio distortion for MMOH stream produced by GW, when live-feed from FXO port is used.

  Conditions: Live-feed is implemented to produce MMOH stream in CME environment, where Live-Feed source is connected to an FXO port. File based Moh also to be configured, and the file needs to be in Cached state.

  Workaround: Remove the file based Moh. Or have a file based Moh which will NOT get cached.

- 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.

- CSCuc53595

  Symptoms: Hung calls on FXO ports where supervisory disconnect is used to disconnect calls.

  Conditions: Analog phone / device initiates disconnect. Custom CPTone is used to detect the disconnect tone that is provided to the FXO port

  Workaround: Configure the analog device to use one of the default CPTones that is bundled with IOS (country based).

- CSCuc53667

  Symptoms: ESP crashes in response to a show command.

  Conditions: When issuing the following show command on a ASR1K 1RU, ESP5, ESP10, ESP20 and ESP40 system.

  show platform hardware qfp [active | standby] infrastructure bqs [schedule|queue] qid

  This only causes an ESP crash when the 'qid' specified is an internal queue. It is safe for interface or QoS created queue.

  Workaround: Avoid use of the show command to display internal queues.

  PSIRT Evaluation:

The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.8 or 3.3:

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

- 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.

- CSCuc67664

  Symptom: Multiple failed IKE negotiations result in multiple MM_KEY_EXCH states from same spoke. The older failed SA's are never deleted from the IKE SA db. This ultimately would exhaust the call admission limit set on the router.

  Conditions: 3945 router running 15.(1)4M5 code.

  Workaround: Staying at 15.1(4)M4 at the moment.

- CSCuc80457

  Symptom: When ASR1K router is equipped with FP100 or FP160 models, the conditional police might fail to work if the physical interface of the tunnel QoS changes to a different one.

  Conditions: If the child policy of tunnel QoS contains "priority <kbps>" and "fair-queue" features, the police of the "priority" feature will fail to function if the physical interface is changed to a different one. Then the priority traffic would behaves like strict priority feature which might starve other traffic class. This issue is specific to certain FP models, like FP100 and FP160.

  Workaround: Detach and reattach the same policy-map to tunnel interface will restore the functionality for Tunnel QoS.

- 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.

- CSCuc95160

  Symptom: After receiving the CRCX message, the Cisco AS5400 does not send 200 ok to SSW. SSW sends the CRCX message to the Cisco AS5400 again. Between these messages, debug outputs are displayed. It seems that the call is not disconnected completely for the end point by the previous disconnect request (the DLCX is received after the CRCX message from SSW). The end point may be stuck in call_disconnecting state. 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.

Conditions: This symptom is observed with MGCP. This issue occurs when the Cisco AS5400 receives DLCX before sending 200 ok for the first CRCX message.

Workaround: There is no workaround.

- CSCud02391

  Symptom: The EIGRP routes are not coming up after removing and reenabling the tunnel interface.

  Conditions: This symptom is observed when EIGRP routes do not populate properly.

  Workaround: There is no workaround.

- CSCud17362

  Symptom: ASR router may crash running under heavy load

  Conditions: This issue is considered an extreme corner case caused by the exhaustion of resources combined with the aggressive polling of information through CLI while the system is overloaded.

  Workaround: There is no workaround.

- CSCud21500

  Symptom: Router crash at speed dial.

  Conditions: This symptom occurs during the speed dial.

  Workaround: There is no workaround.

- CSCud36343

  Symptom: Router crash at speed dial.

  Conditions: This symptom occurs during the speed dial.

  Workaround: There is no workaround.

- CSCud78362

  Symptom: GW starts to drop calls randomly if you increase simultaneous calls beyond 350.

  Conditions: This symptom occurs if 350 calls are connected on GW, some doing digit collection using Cisco ASR(MRCPv2) and some playing media. Increasing a few more calls triggers the issue of call drops and total calls stay at only 350.

  Workaround: A patch was provided which fixed the issue.

- CSCud83835

  Symptom: An IPsec VPN tunnel fails to be established. The **debug crypto ipsec** command shows no output when attempting to bring up the tunnel.

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

  - 1) The crypto map is configured on a Virtual-Template interface.
  - 2) This Virtual-Template interface is configured with "ip address negotiated".
  - 3) The tunnel is initiated locally (in other words, if the tunnel is initiated by the peer, it comes up correctly).

  Workaround: Downgrade to Cisco IOS Release 15.2(2)T3 or earlier releases or always initiate the VPN tunnel from the peer.

- CSCud85342

  Symptom: IKE responder fails to accept phase 1 proposal with rsa-sig authentication with public RSA keys and no trustpoints configured.

Conditions: An authentication mechanism of rsa-sig is configured and rsa-encr cannot be used due to hardware/software limitations.

Workaround: Use rsa-encr if supported, otherwise switch to using actual certificates with trustpoint or pre-shared keys.

- CSCud87915

  Symptom: EzVPN client cannot access the Internet over the VPN. Access to Hub internal resources works fine. The ZBF firewall on the Hub drops the encryptred ESP(udp) traffic from self to out containing reply from the host on the Internet. Log on the hub:

  ```
  *Dec 28 15:34:51.189: %FW-6-DROP_PKT: Dropping udp session 8.8.8.2:0 8.8.8.1:53000 on
  zone-pair self-out class class-default due to  DROP action found in policy-map with ip
  ident 0
  ```

  source IP and port is incorrect.

  Conditions: EzVPN client behind NAT and source port is PATed - is not udp 4500. EzVPN client reaching the Internet with u-turn on the Hub. Hub has ZBF policy from self to outside permitting VPN traffic. Hub has CEF enabled.

  Workaround: Remove the ZBF policy from self to outside.

- 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.

- CSCud88483

  Symptom: In GETVPN and IPSEC redundant configuration combination, if secondary group member is reloaded in the topology, it causes TEK registration of the group member is lost once the router comes back up and HSRP does state transition to standby.

  Conditions: GETVPN with IPSec Redundancy configuration.

  Workaround: Wait for next rekey or issue **clear crypto gdoi**.

- CSCud92596

  Symptom: When traffic is sent with VLAN2 tag between two ixia ports through ASR1004 as below. After executing the command show controller, **input vlan errors** can be found and the counter increases without any packet drops. It is also found that when show interface command is executed, the value of **input errors** counter under related interface is 0.

  Conditions: There is no known condition for this symptom.

  Workaround: There is no workaround.

- CSCud94248

  Symptom: Voice XML Gateway Crashes While Handling SIP Calls - caps nack'ed.

  Conditions: A fax tone getting detected on the gateway is causing the gateway to send a T.38 Fax offer on the SIP leg. However customer does not support fax calls and the gateway receives 400 Bad Request Response for the T.38 Fax Offer. When responding with a ACK for 400 Bad Request Response we are seeing a crash as for some reason ccb->pld.destVdbPtr is getting set to NULL. Accessing the NULL pointer is causing a crash.

  Workaround: Remove the fax configuration in "voice service voip->sip" will prevent the crash.

- CSCud96896

Symptom: "x Calls in queue" status is not displayed on all agents in the hunt group.

Conditions: This happens when a particular agent is logged out, then the subsequent agents (i.e in the order in which they are configured a list member) do not get the status update.

Workaround: Have all the agents logged in.

- CSCue14418

  Symptom: Only single L2TP IPSEC vpn client can connect to vpn when they are behind PAT device even though NAT DEMUX is configured.

  Conditions: VPN clients behind PAT device.

  Workaround: There is no workaround.

- CSCue18003

  Symptom: Packets drop occur when performing a ping from an ASR 1001 console with packets of large size (i.e. several kilobytes).

  Conditions: This issue is specific to the ASR 1001 and requires a burst of data from the Control Plane to the Forwarding Plane such that internal hardware buffers are saturated. Normal processing continues, however, there are drops when the hardware buffer is full.

  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.

- CSCue32707

  Symptom: crypto pki export <> causes crash.

  Conditions: This symptom is observed in when a SUB CA trustpoint is configured and a trustpoint is configured and enrolled to that SUB CA.

  Workaround: If possible, have the trustpoint on a separate box.

- CSCue33313

  Symptom: A Cisco ASR repeatedly produces a "no-input" event despite inputs provided by caller.

  Conditions: The symptom is observed with the following conditions:

  – IOS VXML GW running Cisco IOS Release 15.x.

  – Problem seems to be triggered by a "no-match' event prior to providing

  expected responses.

  Debugs show the following order of events:

  – GW instructs TTS server to say "please say yes or no, or press digits 1 or two".

  – GW instructs ASR to recognize.

  Workaround: There is no workaround.

- CSCue37000

  Symptom: GTP-U drops are noticed for communication that should not have been dropped. Swisscom agrees that this might be related to some timers and pending PDP sessions that need to be terminated. Since local tests with mobile devices are all successful, Swisscom wants and needs to go for 24 hour test to see if the GTP-U drops really lead to a service impact for mobile users.

  Conditions: There is no conditions.

  Workaround: There is no workaround.

- CSCue39518

  Symptom: A Cisco 7200 with VSA fails to encrypt traffic under specific conditions.

  Conditions: The symptom is observed under the following conditions:

  - Cisco 7200 has IPsec SSO configured with HSRP. Dynamic crypto map is
  - configured. Remote sides have static crypto map to this device.
  - All the 15.x codes to the latest Cisco IOS 15.2(4)M2 are affected.
  - Issue is not seen in the Cisco IOS 12.4 codes.
  - Issue not seen when IPsec SSO and HSRP are removed.

  Workaround: There is no workaround.

- CSCue45131

  Symptom: sVTI tunnel interface does not come up after router reboot.

  Conditions: This issue happens when you reboot the router.

  Workaround: Reload ESP.

- 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.

- CSCue48419

  Symptom: The Cisco AS5350 stops processing calls on PRI with a signaling backhaul from PGW. In the packet trace, there is no q931message from PGW. Further analysis shows that as5350 sends a q_hold (0x5)message in BSM, causing peer (PGW) to stop sending signaling traffic. However, there is no BSM_resume message or BSM_reset sent after it. Hence, PGW is stuck in this condition. There was earlier defect for CSCts75818 with similar symptoms in U-state.

  Conditions: This symptom is observed due to some RUDP timing issues that cause BSM session switchover.

  Workaround: Reload the Cisco AS5350 (but only when CU notices the outage). Also, shutting both Ethernet interfaces may help, but this workaround has not been tested.

- 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.

- CSCue52963

Symptom: Some of the SPA goes to *inserted (physical)* state after an ISSU upgrade. This issue is not specific to any particular SPA or SIP.

Conditions: This issue is seen while doing an ISSU upgrade on a setup that has a high scale configuration. Altleast 2000 subinterfaces are configured in the router.

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

- CSCue57374

  Symptom: QFP load spike occurs when dropping traffic via IPv6 ACL.

  Conditions: IPv6 traffic is dropped with ACL.

  Workaround: Configure the **no ipv6 icmp unreachable** command under the receiving interface.

- CSCue57582

  Symptom: The following error message may appear:

  ```
  %STILE_CLIENT-4-MAX_LINK_TOUCH_WARN: F0: cpp_cp: NBAR number of flow-slinks threshold
  is reached, cannot allocate more memory for flow-slinks.
  ```
  This may cause some degradation in SSL based traffic.

  Conditions: This message may appear under heavy SSL traffic.

  Workaround: Currently there is no workaround. The classification of the SSL-based traffic should be based on the other classification mechanisms.

- CSCue59967

  Symptom: VPN led does not come up when an IKEv2 tunnel is active.

  Conditions: IKEv1 is not affected only IKEv2.

  Workaround: There is no workaround.

- CSCue63807

  Symptom: SIP call during "Call Forward No Answer" option leaks the Transcoder resource used on CUBE Example call flow: Telco -> SIP Trunk (G711alaw/G729) -> CME -> SIP phone (G711ulaw) ->NOAN -> CUE (G711ulaw)

  Conditions:

  - SIP Call
  - Codec mis-match between two legs of the call and invokes the local transcoder resource.
  - Call forward No Answer (noan) feature

  Workaround: Reset the sccp session.

- CSCue65405

  Symptom: SAs do not get installed in GETVPN GM.

  Conditions: The symptom is observed when the key server is configured with "receive-only" SAs.

  Workaround: Remove receive-only configuration at the key server.

- 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.

- 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

- CSCue89658

  Symptom: A kernel core file is generated. Process core files that were being generated are incomplete.

  Conditions: The kernel core is generated when HMAN stops strobing the HW Watchdog timer. This occurs concurrently when a process with a large resident set size (IOSd) is dumping core.

  Workaround: There is no workaround.

- CSCue89779

  Symptom: A FlexVPN spoke configured with an inside VRF and front-door VRF may have problems with spoke-to-spoke tunnels if they are not the same. During tunnel negotiation, two virtual-access interfaces are created (while only one is needed), the one in excess may fail to cleanup correctly. As a result, the routes created by NHRP process may lead to loss of traffic, or traffic may continue to flow through the Hub.

  Conditions: This symptom occurs when the VRF used on the overlay (IVRF) and the VRF used on the transport (FVRF) are not the same.

  Workaround: There is no workaround.

- 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
  ```

- CSCue98604

  Symptoms: A Cisco 3845 that is running Cisco IOS Release 15.1(4)M2 may have a processor pool memory leak in CCSIP_SPI_CONTROL.

  Conditions: The conditions are not known at this time.

  Workaround: There is no workaround.

- CSCuf03688

  Symptoms: If the call to transfer-target fails, this problem would occur.

Conditions: When an external Application is registered to UC gateway via a web-services interface,

Workaround: External application is not registered or the registered application do not subscribe for AUTHORIZE_CALL event.

- CSCuf08585

  Symptom: NAT64 does not work in simulator.

  Conditions: This issue is not seen on hardware.

  Workaround: A reboot is likely to clear the issue.

- CSCuf09056

  Symptom: The traffic may not be shaped correctly resulting in more traffic to leak through or the router crashes when model 3/4 subscriber policy is applied.

  Conditions: The model 3 and 4 hierarchy is built incorrectly on ESP-100/200 and ASR1002X when the subscriber policy is added after the main interface is already active.

  Workaround: There is no workaround.

- CSCuf17379

  Symptom: NA

  Conditions: NA

  Workaround: There is no workaround.

- CSCuf20108

  Symptom: Using MRCPv2 on VXML GW for CVP calls to 3rd party ASR, we have found the MRCP Client process is disappearing after a few hundred calls. This causes all future calls to fail until the VXML GW is rebooted.

  A traceback is thrown in the logs at this time, indicating a memory problem.

  ```
  Feb 28 00:23:23.949 JST: %SYS-2-FREEBAD: Attempted to free memory at B0D0B0D, not part
  of buffer pool
  Traceback= 18B57F4z 2C60B0Cz 5B120B3z 4BCA9F6z 2BCCA09z 4C7692Ez 4BCAA8Bz 4C8D03Fz
  4C8EE4Bz 4C85EF2z 4C85D2Fz 4C75A21z
  ```

  Running 'show process' after this traceback shows the MRCP Client process is no longer running.

  Conditions: The issue occurs when a Nuance server abnormally tears down MRCPv2 session in the middle of the call. MRCPv2 is needed to trigger the crash. MRCPv1 does not cause a crash.

  Workaround: Set all sessionTimeout configurations to -1 on the Nuance server (In the NSSserver.cfg file). Use MRCPv1 instead of MRCPv2

- 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.

- CSCuf35314

  Symptom: Operation relying on PKI may start failing when enrolling a new trustpoint to same CA as already existing trustpoint.

  Conditions: First seen with Cisco IOS 15.2(4)M1.

  Workaround: Use **crypto key zeroize pubkey-chain** command.

- CSCuf39338

  Symptom: Running **sh sbc FOO sbe mib mgmmediaaddresstable** on standby causes CLI to hang.

Conditions: When enabled SBC-B2B redundancy.

Workaround: Do not run this command on standby.

- CSCuf39344

  Symptom: In SBC-B2B, after *no attach/attach* an adjacency, calls are rejected with 503 Service Unavailable.

  Conditions: This condition occurs under the following:

  - Config vrf001 on BOX1(ACTIVE) then on BOX2(STANDBY).
  - Config adjacency's vrf and signaling-address, and media-address and vrf, both refer to vrf001.
  - Switch-over.
  - no attach/attach adjacency on BOX2(ACTIVE).
  - Later calls are rejected with 503 Service Unavailable.

  Workaround: Always add or change vrf related SBC config on the same box. More Info:

- CSCuf51539
- CSCuf39344

  Symptom: In some rare situations, EzVPN client routers are seen to have an IKEv1 SA lifetime beyond 24 hours - up to "3 weeks, 3 days". This can lead to unpredictable behavior during IKEv1 phase1 renegotiation, notably this can cause the server to initiate a negotiation which would result in errors and interruptions of service over the VPN.

  Conditions: There is no condition.

  Workaround: There is no workaround.

- CSCuf61640

  Symptom: Tracebacks as follows seen during router bootup:

```
%SYS-2-INTSCHED: 'suspend' at level 2 -Process= "Init",
ipl= 2, pid= 3
-Traceback= 4F6966C 6A708EC 890127C 6B4F924 6B4F7F8 6B4EAAC 6B4F43C 6B4F514 6DD6D4C
6DDB3A8 6A23E50 6A23F18 6A24100 57D3F94 57D42D8 4F701E4

0x4F6966C  ---> process_ok_to_reschedule+288
0x6A708EC  ---> process_suspend+4C
0x890127C  ---> random_fill+248
0x6B4F924  ---> default_entropy_routine+9C
0x6B4F7F8  ---> hardware_entropy_source+CC
0x6B4EAAC  ---> nist_instantiate+78
0x6B4F43C  ---> try_create_rng+1B4
0x6B4F514  ---> nist_rng+34
0x6DD6D4C  ---> cts_sap_get_key_counter+54
0x6DDB3A8  ---> cts_sap_init+C4
0x6A23E50  ---> subsys_init_routine+60
0x6A23F18  ---> subsys_init_class_internal+A8
0x6A24100  ---> subsys_init_class+8C
0x57D3F94  ---> system_init+250
0x57D42D8  ---> init_process+94
0x4F701E4  ---> ppc_process_dispatch+
```

  Conditions: The symptom is observed during router bootup.

  Workaround: There is no workaround.

- CSCuf68548

  Symptom: ccpp_cp_svr and fman_fp cores during mdr.

Conditions: While doing spa/SIP OIR during mdr.

Workaround: There is no workaround.

- CSCuf81742

  Symptom: An ESP crash occurs.

  Conditions: In the rare case, where the software managed memory pools have been increased and a coalescing of buffer pools is required to create large buffers out of smaller buffers. Only a few features (MLPPP, FRF12, ESS, SSL, and IP reassem) make use of this memory.

  Workaround: There is no workaround.

- CSCuf93376

  Symptom: CUBE reloads while testing SDP pass-through with v6.

  Conditions: CUBE reloads while testing SDP pass-through with v6.

  Workaround: Do not use SDP pass-through and use normal SIP processing call flows.

- CSCuf93606

  Symptom: A Cisco 3945E router crashes.

  Conditions: The symptom is observed with the following conditions:

  - Extension mobility is configured for the phone. The logout profile should not
  - be configured with any number.
  - In the logged out state, user has to press the "NewCall" softkey followed by
  - dialing any digit between 1-9 (excluding 0).
  - Instead of pressing "dial" softkey, press "AbbrDial" softkey.

  Workaround: Have a proper number configured under the logout profile.

- CSCug04660

  Symptom: Spurious CPLD-EHSA interrupts are seen. These interrupts are seen in **cmand_R* tracelog** file. Sometimes, these can also cause high CPU depending on the activity on the USB device.

  Conditions: When an external USB device is attached to an Intel-x86 based RP. This includes RP2, 1RU, 2KP platforms. RP1, 2RU, 2RU-F are PPC based platforms, so these do not have this issue. On Intel x86 platforms, CPLD interrupt lines are shared with external USB devices. Spurious CPLD-EHSA interrupts are in fact USB interrupts.

  Workaround: Remove external USB device from the router when not in use.

- CSCug08555

  Symptom: A 3945e will crash due to a bus error with a null instance variable.

  Conditions: This has been observd on a 3945e but the conditions are still unknown.

  Workaround: There is no workaround.

- CSCug09761

  Symptom: Handshake fails when we select Diffie Hellman cipher suite from sslvpn configuration.

  Conditions: There is no condition.

  Workaround: Select other than Diffie Hellman cipher suite at sslvpn.

- 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.

- CSCug18233

  Symptom: Using local ikev2 authorisation policy, it is not possible to push prefix along with the ip address to the client. The prefix always gets pushed as 128.

  Conditions: ikev2 local authorisation.

  Workaround: Use radius server to push the prefix to the client.

- CSCug18685

  Symptom: An NHRP resolution request is forwarded to the first NHS on the tunnel interface instead of being forwarded along the routed path.

  Conditions: DMVPN phase 3 implementation.

  Workaround: Use radius server to push the prefix to the client.

- CSCug19148

  Symptom: FXS ports on a Cisco VG224 running Cisco IOS versions 124-24T7 or 151-4M5 will stop working randomly, user will hear a busy tone when going offhook on the analog device connected to the FXS port on the VG224. The call status will show as "ERR_WAIT4_DISC" or "ERR_WAIT4_ONHO" in the output of the command "show stcapp device summ" for that problematic FXS port.

  Conditions: The Cisco VG224's FXS ports are set up as STCAPP with Cisco Unified Callmanager (CUCM) server and have the shared line feature enabled with a Cisco IP phone on the same CUCM cluster.

  Workaround: Remove the "shared line" feature if feasible or issue a "shut" followed by "no shut" under the problematic FXS voice-port via the VG224's IOS command line interface (CLI) or issue a manual "reload" on the VG224 during a maintenance window.

- CSCug19697

  Symptom: "playout-delay fax" CLI is not changing T.38 and modem Passthrough playout buffer to accommodate packet jitter.

  Conditions: Ability to reduce the default Fax playout delay.

  Workaround: There is no workaround.

- CSCug20669

  Symptom: ASR1000 router crashes due to PPTP related traffic.

  Conditions: Router is running on 3.9.0S. NAT PAT is configured in CGN mode on the router.

  Workaround: Disable PPTP ALG in CGN mode. No ip nat service pptp.

- CSCug21413

  Symptom: Call failure.

  Conditions: Media antitrombone + Call farward cases + SDP passthrough.

  Workaround: There is no workaround.

- CSCug28041

Symptom: In a NAT64 configuration, "show policy-map type inspect zone-pair sessions" shows NATed ipv4 address for the ipv6 host. It should show the hosts' real IP addresses, i.e. v6->v4 or v4->v6, not v4->v4.

The PD command **sh plat ha qf ac fe fir da scb** actually shows the scb's addresses as the real hosts' addresses, i.e. v6->v4 or v4->v6. However, the v6 host's port number is still shown as the translated v4 port number.

In the ZBFW datapath log at cpp_cp*.log, the session key printed in the debug messages is showing wrong port number. The session key is supposed to be all v4, but the port number is actually printed as v6 port number.

For the PD show scb command filter such as **sh plat ha qf ac fe firewall datapath scb ipv6 3000::2 44 ::1d00:2 444**, we can't use the v6 port to match the session and have to use v4 port of the v6 host to match.

Conditions: NAT64 configuration. For the issues involving v6/v4 port numbers, they are only visible if there is PAT configuration, i.e. if the v6 host's port number can be changed after NAT64 translation.

Workaround: There is no workaround.

- CSCug28192

  Symptom: Over-sampling entropy source on Cavium and Quack/ACT based platforms.

  Conditions: There is no condition.

  Workaround: There is no workaround.

- CSCug28631

  Symptom: Silent suppression of the line that is causing the difference in behavior.

  Conditions: Silent suppression of the line that is causing the difference in behavior.

  Workaround: Remove the silent suppression line using the lua script `LVASR01#more bootflash:edit_silence_supp.lua function delete_lines(msg) for line in msg.sdp:select_by_prefix("a=silenceSupp:off"):iter() do line:delete() end end MeEditor.register(MeEditor.BEFORE_RECEIVE,"SilenceSupp",delete_lines).`

- 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.

- CSCug30823

  Symptom: No media forwarded or media dropped for "Reprocess limit exceeded".

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

  - the call is setup as nat call
  - media is received before off/answer completed
  - the call is modified to hairpin with other calls both on two sides

  Workaround: There is no workaround.

- CSCug31076

  Symptom: ASR1000 ESP may get reloaded unexpected when PfR NAT OER integration feature is enabled.

Conditions: When one of the NAT outside interface shuts down administratively with active NAT translations.

Workaround: Disable PfR NAT OER integration feature.

- CSCug33656

  Symptom: When turning off a wccp service or detachin a service from an interface, the memory allocated for wccp is not freed. This can be seen using: **show platform software memory qfp-control-process qfp active | section WCCP**.

  Conditions: None.

  Workaround: There is no workaround.

- CSCug34404

  Symptom: RP_Crash seen at **be_interface_action_remove_old_sadb**

  Conditions: While unconfiguring the 4K svti sessions after the HA test.

  Workaround: There is no workaround.

- CSCug34507

  Symptom: Traffic decrypted on a Cisco ISR G2 series is process switched instead of staying in the CEF path.

  Conditions: The symptom is observed when the hub and/or the spoke are located behind NAT or PAT.

  Workaround: Disable NAT/PAT.

- CSCug34677

  Symptom: Topology: S---asr1k---D1--\ | x.x.x.x/32 ------D2--/ * ISIS, fast-reroute per-prefix configured * LDP on all interfaces * x.x.x.x/32 is reachable via D1 (primary) and D2 (backup) * Sending traffic from S to x.x.x.x * S, D1, and D2 are simulated (Agilent) * Version 15.3(1)S Problem: Upon failing link asr1k-D1 (laser shut on Agilent, equivalent to pulling fiber), FRR is not triggered and traffic flow is restored when ISIS reconverges.

  Conditions: The symptom is observed in IP network and when FRR is enabled and when ethernet interface is one of the primary path and protected path and when plugging out ethernet wire or remote shutdown.

  Workaround: There is no workaround except changing interface type to POS/ATM.

- CSCug34758

  Symptom: Topology: S---asr1k---D1--\ | x.x.x.x/32 ------D2--/ * ISIS, fast-reroute per-prefix configured * LDP on all interfaces * x.x.x.x/32 is reachable via D1 (primary) and D2 (backup) * Sending traffic from S to x.x.x.x * S, D1, and D2 are simulated (Agilent) * Version 15.3(1)S

  Conditions: Upon failing link asr1k-D1 (laser shut on Agilent, equivalent to pulling fiber), asr1k quickly (<50msec) starts forwarding packets (dest x.x.x.x) to D2 (backup), but with D1's advertised label! Only after ISIS converges the packets are forwarded with the correct label (from D2).

  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

- CSCug37242

  Symptom: Router crash due to memory leak.

  Conditions: The symptom is observed with a CME shared line feature configuration.

  Workaround: Disable the shared line feature will avoid memory leak.

- CSCug38023

  Symptom: I/O Leak in the middle/DSPRM buffer pools are observed

  Conditions: Flex DSPs are present.

  Workaround: There is no workaround.

- CSCug40546

  Symptom: QFP reloads and gets stuck in reset loop until pap or cgn configuration.

  Conditions: This occurs when the router is reloading when the following configurations exist: **ip nat setting mode cgn** and **ip nat setting pap**.

  Workaround: Either remove PAP or CGN configuration. A fix is expected in release 3.9.1 and later.

- CSCug41599

  Symptom: VTCP needs to adjust in case 10k h323 resemble packets size are received. Clear DF bit to decrease the impact on MPLS Path Selection and Limit Packet length for assembled h.323 packet to 8K.

  Conditions: The following apply:

  - Send 10K tcp segments from server
  - pmod manipulate the 1st tcp segment into h323 realization format (03 00 length after tcp header)
  - the response src port 80 and dst 1720

  Workaround: Disable h323 alg.

- CSCug43136

  Symptom: After applying the QoS configuration with policy-maps, the configuration is seen in **show running config properly**. However, on checking the QFP, the following is displayed:

  ```
  sh platform hardware qfp active feature qos all output all"  no interfaces are
  configured as QoS target(s)
  ```

  When checking the matching of the packets on the interface, it is displayed as "0".

  Conditions: IOS XE Version: 03.07.01.S.

  Workaround: There is no workaround.

- CSCug44667

  Symptom: CM tone detector being turned ON irrespective of the fax and modem features being disabled.

  Conditions: CM tone detector being turned ON and being reported to the host by the DSP.

  Workaround: There is no workaround.

- CSCug45517

Symptom: Topology: ========= < -----(SIP Trunk A)-----CUBE-----(SIP Trunk B)-----> CUBE is not forwarding the REINVITE message received from Trunk A to the SIP Trunk B when 491 Request Pending is received from SIP Trunk B for the previous SIP transaction.

Conditions: When 491 Request Pending is received.

Workaround: There is no workaround.

- CSCug50844

  Symptom: REq/RES timeout not work as expected.

  Conditions: FW session under heavy traffic 2K create/delete.

  Workaround: Stop the traffic and the timer works

- CSCug53310

  Symptom: ICMP v6 traffic is observed to drop.

  Conditions: ICMP v6 traffic is observed to drop with cxsc configured under the zbfw policy-map. Drops are observed the zone is applied on a DMVPN tunnel.

  Workaround: There is no workaround.

- CSCug53415

  Symptom: %SMC-2-BAD_ID_HW: is output, and SPA is not disabled. SPA should be disabled if authentication fail.

  Conditions: ASR1001 Built-in SPA.

  Workaround: There is no workaround.

- CSCug54468

  Symptom: ASR 1002-X acting as LNS, RP crashes after shutting down the interface that is connecting LAC.

  Conditions: 5000 sessions with per-session QoS. All these sessions are setup on single L2TP tunnel.

  Workaround: There is no workaround.

- CSCug56212

  Symptom: GTPv1 traffic CPP crashed caused by writing protected memory

  Conditions: Landslide LinuxTC ASR5K GGSN LinuxTC introduced packet delay, drop, reproduced, corrupt, reorder between GTP AIC and GGSN. During the GTPv1 traffic, CPP crash is expected, which is caused by protect memory writing.

  Workaround: There is no workaround.

- CSCug56942

  Symptom: CUOM could not process MOSCQEReachedMajorThreshold clear trap from CUBE SP. For MOSCqe alert clear trap, CUBE should not send CurrentLevel Varbind but should send csbQOSAlertCurrentValue Varbind.

  Conditions: This condition occurs when CUBE SP generates clear trap for voice quality alerts.

  Workaround: The code fix is included in CUBE 15.2(4)S4. If earlier CUBE version is used, manually clean the alarm at CUOM after root cause is rectified.

- CSCug58617

  Symptom: Usernames do not show up in CCP Express. Username shows up on a router with default configuration.

  Conditions: The symptom is observed on routers with configurations that break **show run** format.

Workaround: Use default configuration.

- CSCug59775

  Symptom: Running show crypto map.

  Conditions: During high CPU.

  Workaround: There is no workaround.

- CSCug63013

  Symptom: A DMVPN spoke router running 15.2(4)M3 and configured for Dual Hub - Dual DMVPN failover will fail to forward multicast traffic for EIGRP neighbor forming after failing from primary to backup and back to the primary. EIGRP neighbrship will fail to complete and flap on the spoke. The hub will never show any EIGRP neighborship.

  Conditions: DMVPN spoke router running 15.2(4)M3 in Dual Hub - Dual DMVPN scenario and running dynamic routing protocol must failover and failback to the primary tunnel for this to occur.

  Workaround: Removing "ip nhrp map multicast x.x.x.x y.y.y.y" and readding it resolves the problem.

  The issue doesn't exist in 15.2(4)M1.

- CSCug63839

  Symptom: 7301 router running c7301-advipservicesk9-mz.152-4.M3 is experiencing memory leak in Crypto IKMP process particularly on crypto_ikmp_config_send_ack_addr function.

  Conditions: When running 7301 router and connecting EasyVPN through it, causes leak in Crypto IKMP process over time.

  Workaround: Reload the router over a period of time.

- CSCug65636

  Symptom: 7301 router running c7301-advipservicesk9-mz.152-4.M3 is experiencing memory leak in Crypto IKMP process particularly on crypto_ikmp_config_send_ack_addr function.

  Conditions: When running 7301 router and connecting EasyVPN through it, causes leak in Crypto IKMP process over time.

  Workaround: Reload the router over a period of time.

- CSCug68282

  Symptom: ASR1000 RP crash after software upgrade.

  ```
  Apr 20 09:53:01.396: %SYS-3-BADBLOCK: Bad block pointer 3AFDF4B0 -Traceback=
  1#b3d795682537523829953c9aa18e3e0  :10000000 6FCCF4 :10000000 6FD0A0 :10000000
  1F2279C :10000000 1F1C1B0 :10000000 1F3F750 Apr 20 09:53:01.399: %SYS-6-MTRACE:
  mallocfree: addr, pc  33A1E15C,1011798C 33A1E15C,101178CC 33A1E15C,30000060
  4C3A105C,600003E4  4C3A0834,1049C71C 4C3A0834,1049C5FC 4C3A0834,400003FC
  412703FC,125DFF80 Apr 20 09:53:01.399: %SYS-6-MTRACE: mallocfree: addr, pc
  412703FC,300000F6 4C29B4E0,125DFF80 4C29B47C,20005F00 33A1E15C,1011798C
  33A1E15C,101178CC 33A1E15C,30000060 3AAFFF14,154DA6C4 4C1403F4,60000012 Apr 20
  09:53:01.399: %SYS-6-BLKINFO: Corrupted magic value in in-use block blk 3AFDF4B0,
  words 60, alloc 8, InUse, dealloc 0, rfcnt 1 -Traceback=
  1#b3d795682537523829953c9aa18e3e0  :10000000 6FCCF4 :10000000 6FD0A0 :10000000
  1F1D9C4 :10000000 1F227B4 :10000000 1F1C1B0 :10000000 1F3F750 Apr 20 09:53:01.402:
  %SYS-6-MEMDUMP: 0x3AFDF4B0: 0xF8 0x24 0x3C 0x1653EC7C Apr 20 09:53:01.402: %SYS-6-
  MEMDUMP: 0x3AFDF4C0: 0x8 0x8 0x3AFDF38C 0x8000003C Apr 20 09:53:01.402: %SYS-6-
  MEMDUMP: 0x3AFDF4D0: 0x1 0x0 0x1000001 0x3058827C  %Software-forced reload   Exception
  to IOS Thread: Frame pointer 0x30742CC8, PC = 0x87308B4  UNIX-EXT-SIGNAL: Aborted(6),
  Process = Check heaps -Traceback= 1#b3d795682537523829953c9aa18e3e0  c:86FA000 368B4
  c:86FA000 368B4 c:86FA000 384C8 :10000000 32FD91C :10000000 1F227BC :10000000 1F1C1B0
  :10000000 1F3F750   Fastpath Thread backtrace:  -Traceback=
  ```

```
1#b3d795682537523829953c9aa18e3e0  c:86FA000 D9F08 c:86FA000 D9EE8 iosd_unix:887E000
1580C pthread:7DB2000 5A4C   Auxiliary Thread backtrace:  -Traceback=
1#b3d795682537523829953c9aa18e3e0  pthread:7DB2000 B598 pthread:7DB2000 B578
c:86FA000 EF9C4 iosd_unix:887E000 212F4 pthread:7DB2000 5A4C   PC  = 0x087308B4  LR  =
0x08732384  MSR = 0x0002D000 CTR = 0x07DC0D60  XER = 0x20000000 R0  = 0x000000FA  R1
= 0x30742CC8  R2  = 0x30085C70  R3  = 0x00000000 R4  = 0x00006908  R5  = 0x00000006
R6  = 0x00000000  R7  = 0x08730B5C R8  = 0x0002D000  R9  = 0x3007E7F0  R10 =
0x3007E7F0  R11 = 0x30742CA0 R12 = 0x08732384  R13 = 0x18456078  R14 = 0x11F3F604  R15
= 0x00000000 R16 = 0x00000000  R17 = 0x00000000  R18 = 0x00000000  R19 = 0x00000000
R20 = 0x00000000  R21 = 0x1630C7D8  R22 = 0x18BDAA28  R23 = 0x18BDAC70 R24 =
0x18BDB3B8  R25 = 0xAB1234AB  R26 = 0xAB1234CD  R27 = 0x30742E58 R28 = 0x3AFDF4E0  R29
= 0x30742CE0  R30 = 0x0886A7AC  R31 = 0x00000006   ========= Start of Crashinfo
Collection (09:53:01 UTC Sat Apr 20 2013) =========  For image: Cisco IOS Software,
IOS-XE Software (PPC_LINUX_IOSD-ADVIPSERVICESK9-M), Version 15.2(4)S1, RELEASE
SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-
2012 by Cisco Systems, Inc. Compiled Sat 06-Oct-12 11:55 by mcpre   Uptime = 00:02:51
```

Conditions: Device configured with SBC with interchassis redundancy.

```
redundancy mode none application redundancy   group 1    name ECS    preempt
priority 150 failover threshold 100    timers delay 100    control Port-channel30.8
protocol 1    data Port-channel30.9    track 1 decrement 200    track 2 decrement 200
protocol 1    name BFD    timers hellotime msec 250 holdtime msec 1000.
```

Workaround: Do not setup B2B redundancy between XE36(or older) and XE37(or later).

- CSCug69049

  Symptom: ESP fails to initialize and reboots. A message like the following will be seen on the IOS console:

  ```
  *Jan 01 16:22:35.562: %CPPHA-3-INITFAIL: F0: cpp_ha:  CPP 0 initialization failed -
  startup init (0x1)
  *Jan 01 16:22:35.562: %CPPHA-3-INITFAIL: F0: cpp_ha:  CPP 0 initialization failed -
  start CPP (0x1)
  ```

  The cpp_driver tracelog contains an entry indicating the Hoover PLL failed to lock. This could be on CIF,FIF, or ICM. Here is an example from CIF:

  ```
  01/01 16:22:35.120 [cpp-drv]: (ERR): COMP0053/CIF/1028: QFP0.0 - timeout waiting
  for Hoover TX PLL to lock.
  ```

  Conditions: Router configuration or traffic pattern does not affect this problem. This software error is fixed in to XE3.7.4, XE3.9.2, XE3.10.0 and later releases.

  Workaround: There is no workaround.

- CSCug69540

  Symptom: ESP fails to initialize and reboots. Cman-fp indicates error due to Hoover PLL lock failure.

  Conditions: Router configuration or traffic pattern does not affect this problem. This software error is fixed in to XE3.7.4, XE3.9.2, XE3.10.0 and later releases.

  Workaround: There is no workaround.

- CSCug72874

  Symptom:Group Member is regitering the third Key Server in its list in a redundant KS scenario, when certificate of first KS has been revoked.

  Conditions: This has been observed under the following conditions:

  - GM has a list of 3 or more Key server
  - Certificate based authentication with OCSP validation
  - First KS certificate has been revoked.

Workaround: There is no workaround.

- CSCug73374

  Symptom: ASR 1001 prints following error messages and crashes: % Internal error: Connection to peer process lost %MCP_SYS-0-ASSERTION_FAILED: SIP0: cmcc: Assertion failed: Assertion failed: cman/cc/./src/cmcc_util.c:322: "bay < cmcc_max_spas_per_cc()".

  Conditions: Issue **show platform hardware subslot 0/3 plim statistics** command in CLI.

  Workaround: Not issuing **show platform hardware subslot 0/3 plim** command will avoid this problem.

- CSCug77988

  Symptom: ZBFW syslog for passing and dropping ICMPv6 packets shows wrong value in the port number fields. The src/dst port numbers should be the ICMP type and code. In addition, the passing syslog is showing "Passing Unknown L4 protocol".

  Conditions: The router is configured in 66, 64 or 46 case. syslog for pass or drop logging is enabled. Sending ICMPv6(or ICMP from v4 side) packets.

  Workaround: Not issuing **show platform hardware subslot 0/3 plim** command will avoid this problem.

- CSCug80427

  Symptom: Bursty shape rate on high bandwidth queue.

  Conditions: When there are 2 vlans configured each with a single simple shape queue, one with a very high rate (ex. 400,000,000bps) and another with a very low rate (ex 128,000bps), the high rate queue's rate may be bursty and fluctuate +- 10% of the configured rate.

  Workaround: Configure a hierarchical policymap on the vlans where the shape is on the parent class, not on the queue.

- CSCug82610

  Symptom: NAT translations could be stranded on the standby with NAT B2B and AR configuration.

  Conditions: NAT translations could be stranded on the standby with timeout of zero.

  Workaround: During a MW or downtime, execute the **clear ip nat trans** command on the active box.

- CSCug83538

  Symptom: Static routes injected through RRI (reverse-route static) are not getting removed.

  Conditions: This symptom is observed when a static crypto map that has "reverse-route static" enabled is applied on two different interfaces with a local-address.

  Workaround: Reload the Router.

- CSCug84396

  Symptom: May 3 12:46:21.835: %SYS-2-FREEFREE: Attempted to free unassigned memory at 3EC4FF9C, alloc 350B5A70, dealloc 350B5608

  ```
  -Traceback= 35D9BEC4z 350C158Cz 350AEED8z 350B081Cz 32C23084z 32C23068z
  May  3 12:46:21.839: %SYS-6-MEMDUMP: 0x3EC4FF7C: 0x350B5A70 0x3EC50C58 0x3EC4FDF0
  0x65E
  May  3 12:46:21.839: %SYS-6-MEMDUMP: 0x3EC4FF8C: 0x0 0x350B5608 0x1000133
  0x3CDD2E48%Software-forced reload
  -Traceback= 0x30DF22BCz 0x30DF05F0z 0x32C3278Cz 0x35D9BEC4z 0x350C158Cz 0x350AEED8z
  0x350B081Cz 0x32C23084z 0x32C23068z
  ```

  Conditions: May be with Presence or Shared line feature.

  Workaround: There is no workaround.

- CSCug86085

  Symptom: SBC SRTP ucode crash when doing srtp-rtp interworking.

  Conditions: It seems this can happen in hairpined SRTP calls, though not able to reproduce in the lab. The test scenario is: rtp----SBC-----SRTP--------SBC-------rtp

  Workaround: There is no workaround.

- CSCug86432

  Symptom: Incorrect statistic from SNMP OID "1.3.6.1.4.1.9.9.171.1.3.1.1", related to a number of IPSec tunnels after running "clear crypto sa / session" command.

  Conditions: Configured DMVPN, running "clear crypto sa / session" command.

  Workaround: Reloadof router helps to solve the issue

- CSCug88265

  Symptom: Memory leak in [pfr_config].

  Conditions: Performance Routing (PFR) is configured on the router.

  Workaround: There is no workaround.

- CSCug91165

  Symptom: ESP may reload when switching classic to CGN mode.

  Conditions: ESP may reload when switching classic to CGN mode with traffic.

  Workaround: There is no workaround.

- CSCug92464

  Symptom: NAT timeout when used with port command does not work as expected.

  Conditions: IP NAT translation port-timeout tcp <port #> <timeout value> Above CLI with **ip nat translation tcp-timeout** *timeout value* is used.

  Workaround: Make use of just **ip nat translation tcp-timeout** *timeout value* command.

- CSCug95864

  Symptom: The router crashes when removing and re-attaching a child policy from/to the parent or when removing and re-adding the fair-queue policy. The issue does not require traffic in the background. It could occur with a policy on a single target, so scaling is not required to hit the problem. It happens primarily on ESP-100, ASR1002-X and 1NG (Nightster). The issue does not impact ESP-5, ESP-10, ESP-20 and ESP-40, ASR1001 and ASR1002. The issue does also NOT impact the ISR and CSR platforms.

  Conditions: When removing and re-applying a child policy or a policy that includes fair-queue, the hierarchy grows by one layer each time the policy is re-adding. This result is broken functionality and removing the policy would eventually result into a crash.

  Workaround: The workaround is to remove the parent policy, modify the configuration then re-apply the service policy. The issue could also occur dynamically when a subscribe signs off but there is no workaround for this issue in that case.

- CSCug98010

  Symptom: Crash seen on Primary RP due to Null Pointer send during Bulk Policy Map delete.

  Conditions: Deleting Bulk Cos Policies.

  Workaround: There is no workaround.

- CSCug98593

Symptom: When the ZBFW SYN cookie protection feature is enabled and is being triggered, the firewall will generate and send SYN packets to the server on behalf of the client. If the response from the server isn't received in time, the firewall will re-generate and resend the SYN packet. In this retransmitted SYN packet, the MSS option is missing and the sequence number is incorrect(it is one number bigger than the ISN).

Conditions: ZBFW SYN cookie protection is configured and is being triggered. Server doesn't respond in time and is causing the firewall to resend the SYN packet to the server.

Workaround: There is no workaround.

- CSCug98723

  Symptom: The TCP RST packets generated by ZBFW are dropped by ZBFW on ASR box.

  Conditions: TCP flow specific TCP RST packets generated by ASR to rset the connection to the client and server when "TCP packet inspection" is on.

  Workaround: There is no workaround.

- CSCug98820

  Symptom: Multicast RP-Announcement or RP-Advertisement packet is replicated more than one copy per incoming packet. The number of copies is equal to the number of interfaces or io items with IC flag enabled (use the **show ip mfib** command to get the number of IC interfaces).

  Conditions: AUTO-RP filter is configured on PIM interfaces.

  Workaround: There is no workaround.

- CSCuh01007

  Symptom: After ESP 100 reload, **show policy-map interface** command counters does not populate results.

  Conditions: This condition occurs with an egress service policy on SPA Gigabit Ethernet interface and sending high or low priority traffic.

  Workaround: Reload the SPA after FP reload.

- CSCuh03859

  Sympt om: If a customer configured **snmp server enable traps sbc sla-violation-rev1** csbSLAViolationRev1 trap is not sent.

  Conditions: This is a normal operation.

  Workaround: There is no workaround.

- CSCuh04018

  Sympt om: FMAN-FP traceback: cgm begin batch error.

  Conditions: While adding classes to the ZBFW policy.

  Workaround: There is no workaround.

- CSCuh09403

  Symptom: ESP may reload in B2B NAT ZBFW setup.

  Conditions: B2B NAT ZBFW setup with stateful traffic.

  Workaround: There is no workaround.

- CSCuh09451

  Symptom: Exception to IOS Thread: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SBC main process.

Conditions: There is no workaround.

- CSCuh11874

  Symptom: The ASR1002-X Router reloads with core file reporting CGI_CSR32_CGI_OTHER_LEAF_INT__INT_ECSR_PROTOCOL_ERR interrupt.

  Conditions: Only applies to the ASR1002-X Router. This software error is fixed in the IOS XE3.7.4, XE3.9.2, XE3.10.0 and later releases.

  Workaround: There is no workaround.

- CSCuh12245

  Symptom: cpp_cp process crashes.

  Conditions: Change to the parent class of a session, which causes a rate update event to be performed in the QFP hardware. At the same time, ANCP causes rate change on a VLAN shapper using mode-F QoS. The shaper rate change causes the shaper on the VLAN to be removed and then re-applied. Depending upon RP and FP CPU utilization, these events can be processed on the ESP as one QoS transaction. where the sessions parent class has a rate change event and the session is also being moved to an aggregation schedule node on the GE from the VLAN shaper schedule node. And then the shaper is re-applied to the VLAN and the session is moved back to the VLAN shaper. This all occurs in the same QoS transaction/commit on the ESP, causing the ESP to crash.

  Workaround: There is no workaround.

- CSCuh17401

  Symptom: NAT pool exhaustion with addresses with 0 refcount.

  Conditions: This condition occurs while running NAT ALG and when port allocation failure occurs.

  Workaround: To recover, execute **clear ip nat trans** command in off hours (as this is disruptive operation).

- CSCuh19209

  Symptom: **show ip wccp** counters are not updated

  Conditions: Configure more than 7 services on interface; disable some services; send traffic which match the last configured service;

  Workaround: When disabling service, also delete the configuration on interface.

- CSCuh22742

  Symptom: Callflow: Verizon - SIP trunk - CUBE (ASR 1000) - CUSP - Genesys - Interactions IVR.

  CUBE does not ACK and BYE (glare handling case) after sending Cancel and receiving 200 Ok for cancel from CUSP.

  Conditions: Verizon cancelled the call 300 milliseconds (aprox) after sending the invite, it caused the 200Ok of the invite and the Cancel to cross wire between CUSP and Genesy.

  By that time CUSP had already sent 200 Ok for CANCEL to CUBE, thus CUBE did not respond to the following 200 OK (for Invite).

  Workaround: There is no workaround.

- CSCuh29716

  Symptom: Call flow: Verizon -- CUBE -- CUSP -- Genesys/IVR, transfered with SIP Refer back to PSTN hair-pining the call on CUBE.

  When the call is transferred from IVR to PSTN, the codec negotiation with verizon fails, only if the original Invite received included fax capabilities, dropping the call with reason code 47 and hanging the UDP port used.

All subsequent calls that try to re-use the same UDP port for RTP stream are dropped with reason code 47 and provisn RSP fail is logged on show voip fpi stats

Conditions: Hair-pinned calls that received FAX capabilities on original SIP invite from Verizon.

Workaround: There is no workaround.

- CSCuh33069

  Symptom: qfp crash

  Conditions: handoff from gtpv0 to gtpv1

  Workaround: no More Info:

- CSCuh36750

  Symptom: ESP crashes.

  Conditions: Subscriber session with QoS over tunnel or shaped VLAN.

  Workaround: There is no workaround.

- CSCuh38488

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

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

  Conditions: Application (L7) inspection for SIP must be enabled for the flow.

  Workaround: Any of the following workarounds are applicable:

  - Disable the port-to-application mapping for SIP with the **no ip port-map sip port udp 5060** command. This prevents ZBF from treating UDP/5060 as SIP. Instead, it is treated as simple UDP.
  - Use the *pass* action in both directions instead of *inspect*. This disables all inspection (even L4) for the traffic.

- CSCuh43018

  Symptom: QFP reloads.

  Conditions: Rarely occurs when issuing **show platform hard qfp active feature nat da stats** command. Most likely to occur in CGN mode specifically after switching from classic to CGN mode.

  Workaround: There is no workaround.

- CSCuh44888

  Symptom: PBHK update failure traceback from CPP-CP. AOM object download failure from FMAN-FP..

  Conditions: ISG sessions have PBHK features and RP switch-over.

  Workaround: There is no workaround.

- CSCuh46031

  Symptom: The Cisco ASR 1000 Series Aggregation Services Router sends a different Acct-Session-Id in the Access-Request and Accounting-Request for the same user.

  Conditions: Flex VPN IPSEC remote access is configured.

Workaround: There is no workaround.

- CSCuh50125

  Symptom: ESP crashes.

  Conditions: On ASR1002-X, ESP100 or ESP200 based platforms, ESP can crash when you have interfaces where the bandwidth can change dynamically and you have a hierarchical QoS policy-map applied.

  Workaround: When applying a hierarchical QoS policy-map to ain interface that supports dynamic bandwidth changes, be sure to apply the QoS policy while there are no bandwidth changes to the interface at the same time.

- CSCuh51400

  Symptom: gtpv0 policy is not working.

  Conditions: gtpv0 traffic.

  Workaround: There is no workaround.

- CSCuh58209

  Symptoms: ESP crashes in response to a show command.

  Conditions: This only causes an ESP crash when the **qid** specified is an internal queue. It is safe for interface or QoS-created queue. When issuing the **show platform hardware qfp [active | standby] infrastructure bqs [schedule | queue] qid** command on a ASR1K 1002X, ESP100/FP100, and ESP200/FP200 system.

  Workaround: Avoid use of the show command to display internal queues.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.8/3.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:S/C:N/I:N/A:C/E:F/RL:OF/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

- CSCuh62307

  Symptom: Cisco ASR 1000 Series Aggregation Services Router may crash when customer uses **call-policy-set copy source** *source-address* **destination** *destination-address* command to create a new call-policy-set.

  Conditions: The **na-src-address-table** is configured within the call-policy-set. Enter this table with **na-src-address-table XXX** after it was created by **call-policy-set copy** command.

  Workaround: instead of using **call-policy-set copy source** *source-address* **destination** *destination-address* command, copy and paste the text into config terminal to create a new call-policy-set.

- CSCuh75480

  Symptom: QFP reload may occur.

  Conditions: When running NAT in CGN mode and doing a removal of a mapping.

  Workaround: Switch to classic mode, to mapping removal, switch back to CGN mode.

- CSCuh76529

  Symptom: Unknown.

Conditions: Astro can require a core voltage of up to 1.00V. However, the voltage was defaulted to 0.9V for all Astro chips. If an Astro requires 1.0V is on a board, it is only operating at 0.9V and could fail to operate properly at speed.

Workaround: There is no workaround.

- CSCuh85883

  Symptom: mplssetvrf bgp routes are not coming up along with multi-vrf PBR.

  Conditions: The destination address of the packet is ASR local address. Say, the packet is for us packet.

  Workaround: There is no workaround.

- CSCuh91266

  Symptom: VTCP is not robust enough when it receives TCP segments with abnormal sequence ID. This may result in FP crash. We observed a TCP packet much older than the current window on customer network.

  Conditions: Abnormal sequenced TCP segments are received when VTCP buffering current flows.

  Workaround: There is no workaround.

- CSCuh93698

  Symptom: The Calling-Station-Id is not sent in the accounting-request.

  Conditions: Easy VPN server or Flex VPN remote access is configured along with the "radius-server attribute 31 remote-id" command.

  Workaround: There is no workaround.

- CSCuh95125

  Symptom: ESP-100 may crash continuously on an ASR1K box with cpp_svr crashes causing the FP to go down.

  Conditions: Numerous QoS sessions with a single queue being created on an interface in a per-session basis on a Yoda platform (ASR1002-X/ESP100/ESP200).

  Workaround: None at the moment More Info: This bug only affects Yoda platforms with large number of singe queued QoS policies being applied on a per session basis on an interface.

- CSCui06926

  Symptom:

  - Initiator sends identity certificate based on 'ca trustpoint' under the
  - isakmp-profile.
  - However, the responder does not do this. Instead it gets the identity certificate from the *first* trustpoint (out of the list of trustpoints) based on peer's cert_req payload in MM3.

  Conditions:

  - IKEv1 with RSA-SIg Authentication, where each Peer has two certificates issued by the same CA.
  - Each Peer has isakmp profiles defined that match on certificate-map and have 'ca trustpoint' statements with self-identity as fqdn.

  Workaround: There is no workaround.

- CSCui24927

Symptom: Data rate for a QoS shaped MLPPPoA/MLPPPoEoA traffic class may exceed the configured QoS shape rate.

Conditions: This issue will be apparent if a parent or child shaper is defined on the MLPPP bundle interface that is less than the configured PVC data rate.

Workaround: The user can explicitly tell the shaper to account for the ATM Cell Overhead by appending the "account user-defined 0 atm" configuration option to the shaper configuration.

Example:

shape rate *rate* **account user-defined 0 atm**

Note that if the session is already active when modifying the QoS policy-map, the session may need to be restarted for the QoS modification to take affect.

This issue will be addressed in the upcoming XE3.8, XE3.10, and later releases. This issue will not be addressed in XE3.8 and XE3.9 and will require migration to XE3.10 or later releases to pick up this fix when available.

- CSCui26458

  Symptom: Call flow: **Verizon -- CUBE -- CUSP -- Genesys/IVR**, transfered with SIP Refer back to PSTN hair-pining the call on CUBE. When the call is put on hold to be transferred from IVR to PSTN, the CODEC negotiation fails, dropping the call with reason code 47 and hanging the UDP port used. All the subsequent calls that try to reuse the same UDP port for RTP stream are dropped with reason code 47 and provison RSP failure is logged on **show voip fpi stats** command.

  Conditions: Hair-pinned calls that receive multiple M-Lines on the SDP received from Verizon on the original SIP Invite.

  Workaround: There is no workaround. Reload of router is required to clear hung UDP ports.

- CSCui27725

  Symptom: When ASR1000 connect with ISO HDLC equipment, the ATOM PW traffic could not transparent successfully.

  Conditions: In L2VPN ATOM PW configuration, AC on the PE is CISCO HDLC encapsulation, and CE equipment is ISO HDLC.

  Workaround:

  – CE configure CISCO HDLC.

  – CE configure as the FR, and PE configure as HDLC.

- CSCui38316

  Symptom: The ESP crashes when updating a highly scaling configuration with a large number of flow-controllable nodes. The crash could be observed during dynamic reconfigurations such as changing the rates of a scheduling node, e.g. an ATM VC due to changing L2 shaping or QOS via MQC.

  The crash could also occur due to growing a scheduling node or moving an ATM VC from one class-of-service node to another.

  There are several other scenarios that could lead to a transformation of a hierarchy in order to lay out the tree correctly to meet the hardware requirements. One such example is applying a flat policy to or removing a child policy from a policy attached to an ATM VC.

  Conditions: While transforming a hierarchy, there are hardware primitives used to execute the update logic safely. One of requirements for this procedure is to move flow-control from the old tree to the new tree in a particular order to prevent packets from getting out of order. The BQS resource manager had a bug that caused the update to deplete internal flow-control IDs.

Workaround: There is no workaround.

- CSCui49230

  Symptom: After reloading ASR1k with redundancy RP/FP, HDLC pass through configuration remains but control flag actually lost.

  Conditions: ASR1k with redundancy RP/ESP Configured HDLC pass-through and reload, or FP switchover for two times.

  Workaround: Manually re-config the CLI after reload.

```
UUT-ASR2-1006HA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
UUT-ASR2-1006HA(config)#platform l2vpn hdlc-pass-through
UUT-ASR2-1006HA#sh plat hard qfp ac fea xcon cli intern
Platform Xconnect global configuration
L2VPN HDLC pass through control flag: TRUE
```

- CSCui55732

  Symptom: ASR1k:support of ignore-dtr on 4XT-Serial spa.

  Conditions: There is no condition.

  Workaround: There is no workaround.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.3S

This chapter contains the following sections:

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.3S

This section documents the unexpected behavior that might be seen in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.3S.

- CSCtz49200

  Symptom: OSPF IPv6 control packets are not encrypted or decrypted.

  Conditions: This issue occurs while configuring the IPv6 OSPF authentication.

  Workaround: There is no workaround.

- CSCua90097

  Symptom: flexVPN client ikev2 sa stuck at IN-NEG with status description: `Initiator waiting for AUTH response.`

  Conditions: flexVPN server initial **`clear crypto session`** command to clear 4K crypto sessions. After crypto session recovered, there is 1 ikev2 sa at flexVPN client stuck at IN-NEG status. At flexVPN server, there is no ikev2 peer, 172.4.234.1.

```
Client: 2ru-2#sh crypto ikev2 sa local 172.4.234.1 det
```

```
Load for five secs: 12%/1%; one minute: 9%; five minutes: 9%
Time source is NTP, 11:49:38.299 PDT Thu Jul 5 2012
Tunnel-id Local         Remote              fvrf/ivrf    Status   1
172.4.234.1/500       172.255.255.252/500   none/none    IN-NEG
Encr: AES-CBC,   keysize: 256,   Hash: SHA512,  DH Grp:5,    Auth sign: PSK, Auth
verify: Unknown - 0    Life/Active Time: 86400/0 sec      CE id: 50798, Session-id: 0
Status Description: Initiator waiting for AUTH response
Local spi: 7E92CB576E3BC65B       Remote spi: 01B87002CE230A4A
Local id: 2ru-2-1000.cisco.com       Remote id:        Local req msg id:  1
Remote req msg id:  0                 Local next msg id: 2
Remote next msg id: 0                 Local req queued:  1
Remote req queued:  0                 Local window:      5
Remote window:   1             DPD configured for 0 seconds, retry 0
NAT-T is not detected          Cisco Trust Security SGT is disabled       Initiator
of SA : Yes     2ru-2#
```

Workaround: flexVPN client is able to use the **clear crypto ikev2 sa psh <index>** command to delete stuck ikev2 sa.

- 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.

- CSCud41480

  Symptom: QFP may reload.

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

  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.

- 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.

- 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.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.3S

This section documents resolved issues on Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.3S.

- CSCsr06399

  Symptom: A Cisco 5400XM may reload unexpectedly.

  Conditions: This symptom is intermittent and is seen only when the DSPs available are insufficient to support the number of calls.

  Workaround: Ensure that sufficient DSPs are available for transcoding.

- CSCtq41512

  Symptoms: After reload, ISDN layer 1 shows as deactivated. Shut/no shut brings the PRI layer 1 to Active and layer 2 to Multi-frame established.

  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.

- CSCtu02543

  Symptom: Sometimes, users may face a "peer leak" situation with EzVPN.

  Conditions: This symptom may occur when an NAT box gets reloaded/rebooted with live translations.

  Workaround: Reload the router to clear the leaked peers.

- CSCty31905

  Symptom: The router crashes upon initiation of an MSRPC secondary channel.

Conditions: When using a pre-gen created by control channel.

Workaround: There is no workaround.

- CSCty61216

  Symptom: When the system includes a Cisco AS5350 universal gateway, the CCSIP_SPI control causes a memory leak.

  Conditions: The symptom is observed with the following IOS image: c5350-jk9su2_ivs-mz.151-4.M2.bin. It is seen with an outgoing SIP call from gateway (ISDN PRI --> AS5350 --> SIP --> Provider SIP gateway).

  Workaround: There is no workaround.

- CSCtz15274

  Symptom: When attempting a T.38 fax call on a gateway, you might see the following in the logs: 006902: %FLEXDSPRM-3-UNSUPPORTED_CODEC: codec cisco is not supported on dsp 0/0 006903: %FLEXDSPRM-5-OUT_OF_RESOURCES: No dsps found either locally or globally.

  Conditions: The symptom is observed with a T.38 fax call.

  Workaround: There is no workaround.

- CSCtz21456

  Symptom: A router has an unexpected reload due to CCSIP_SPI_CONTROL process.

  Conditions: This issue has been seen in Cisco IOS Release 15.2(3)T.

  Workaround: There is no workaround.

- CSCtz55145

  Symptom: Files cannot be downloaded using the management interface via FTP or HTTP. SCP might also be affected. This can include firmware files, configuration files, or license files.

  Conditions: This symptom occurs when using the management interface on a RP2 route processor or the Cisco ASR 1000 router.

  Workaround: Use an interface other than the management interface to download the file or use a protocol that does not use TCP as the session transport, for example, TFTP. If you need to use the management interface, see the workaround attached to the caveat.

- CSCtz78943

  Symptom: A Cisco router experiences a spurious access or a crash. Cisco ISR-G1 routers such as a 1800/2800/3800 experience a spurious access. ISR-G2 routers such as the Cisco 2900/3900 routers that use a Power PC processor crash because they do not handle spurious accesses.

  Conditions: This symptom occurs after enabling a crypto map on an HSRP-enabled interface.

  Workaround: There is no workaround

- CSCua10477

  Symptom: The ASR1002-X Series Aggregation Services Router with large numbers of MLPPP bundles might experience a crash, with the following error message: `%CPPOSLIB-3-ERROR_NOTIFY: SIP0: cpp_cp: cpp_cp encountered an error.` This would be followed by a traceback and eventual reload of the router.

  Conditions: Large numbers MLPPP bundles on an ASR1002-X Series router.

  Workaround: Keep the number of single-link MLPPP bundles under 4000, and the total number of multi-member MLPPP bundles under 2000.

- CSCua31157

  Symptom: (Intermittently) One-way traffic is seen on a DMVPN spoke-to-spoke tunnel one minute after the tunnel is built. Message: `Invalid SPI`.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T1.

  Workaround: There is no workaround.

- CSCua42104

  Symptoms: Malformed RTCP packets are observed.

  Conditions: This symptom occurs when DTMF interworking is enabled or SRTP/SRTCP is in use.

  Workaround: Disable DTMF interworking if not required for the call.

- CSCua49764

  Symptom: The WAAS-Express device goes offline on WCM.

  Conditions: This symptom occurs when a certificate is generated using HTTPS using the Cisco IOS Release 15.1(3)T image. After upgrade to Cisco IOS Release 15.2(3)T, the WAAS-Express device goes offline on WCM.

  Workaround: Configure an rsakeypair on the TP-self-signed trustpoint with the same name and execute the `<CmdBold>enroll<noCmdBold>` command again or delete the self-signed trustpoint point and reenable the HTTP secure-server.

- CSCua55629

  Symptom: SIP memory leak seen in the event SIPSPI_EV_CC_MEDIA_EVENT.

  Conditions: The command **show memory debug leaks** shows a CCSIP _SPI_CONTORL leak with size of 6128 and points to the event:

```
SIPSPI_EV_CC_MEDIA_EVENT?:
Adding blocks for GD...
                  I/O memory
Address     Size   Alloc_pc  PID   Alloc-Proc       Name
                    Processor memory
Address     Size   Alloc_pc  PID   Alloc-Proc        Name
286E144     6128   8091528   398   CCSIP_SPI_CONTR   CCSIP_SPI_CONTROL
```

  Workaround: There is no workaround.

- CSCub05907

  Symptoms: Reverse routes are not installed for an IPsec session while using dynamic crypto map.

  Conditions: Occurs when the remote peer uses two or more IP addresses to connect and the session goes down and comes back at least twice.

  Workaround: Issue **clear crypto session** for that peer.

- CSCub14044

  Symptom: A crash with traceback is seen, and all calls are dropped.

  Conditions: This symptom is observed under all conditions.

  Workaround: There is no workaround. The gateway crashes, and the soak time appears to be six weeks.

- CSCub42181

Symptom: The router crashes continuously after a normal reboot due to power or some other reason. Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M4, RELEASE SOFTWARE (fc1) uptime is 4 days, 11 hours, 38 minutes System returned to ROM by error - a Software forced crash, PC 0x88D26F0 at 07:42:45 UTC Sat May 5 2012 System restarted at 07:43:55 UTC Sat May 5 2012 System image file is `"flash:c3900-universalk9-mz.SPA.150-1.M4.bin" ; Last reload type: Normal Reload ---------- generated Traceback: Pre Hardware Replacement Crashinfo: ---------- #more flash0:crashinfo_20120519-165015-UTC ---------- Traceback Decode: ---------- tshakil@last-call-2% rsym c3900-universalk9-mz.150-1.M4.symbols.gz Uncompressing and reading c3900-universalk9-mz.150-1.M4.symbols.gz via /router/bin/zcat c3900-universalk9-mz.150-1.M4.symbols.gz read in Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z 0x88D1D88:fsm_crank(0x88d1d2c) 0x5c 0x88D27C0:fsm_exec_w_option(0x88d2650) 0x170 0x729E558:htsp_process_event(0x729e1d4) 0x384 0x729E6F4:htsp_main(0x729e62c) 0xc8 0x495F298:ppc_process_dispatch(0x495f274) 0x24 0x4962FC8:process_execute(0x4962e24) 0x1a4 Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z 0x88D1D88:fsm_crank(0x88d1d2c) 0x5c 0x88D27C0:fsm_exec_w_option(0x88d2650) 0x170 0x729E558:htsp_process_event(0x729e1d4) 0x384 0x729E6F4:htsp_main(0x729e62c) 0xc8 0x495F298:ppc_process_dispatch(0x495f274) 0x24 0x4962FC8:process_execute(0x4962e24) 0x1a4 Enter hex value: ---------- Crash File Post Installation: ---------- #more flash0:crashinfo_20120519-185725-UTC ---------- Traceback Decode: ---------- Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z 0x88D1D88:fsm_crank(0x88d1d2c) 0x5c 0x88D27C0:fsm_exec_w_option(0x88d2650) 0x170 0x729E558:htsp_process_event(0x729e1d4) 0x384 0x729E6F4:htsp_main(0x729e62c) 0xc8 0x495F298:ppc_process_dispatch(0x495f274) 0x24 0x4962FC8:process_execute(0x4962e24) 0x1a4 Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z 0x88D1D88:fsm_crank(0x88d1d2c) 0x5c 0x88D27C0:fsm_exec_w_option(0x88d2650) 0x170 0x729E558:htsp_process_event(0x729e1d4) 0x384 0x729E6F4:htsp_main(0x729e62c) 0xc8 0x495F298:ppc_process_dispatch(0x495f274) 0x24 0x4962FC8:process_execute(0x4962e24) 0x1a4 ----------`

Conditions: This symptom is observed with the following conditions: - MGCP gateway. - Take out all the modules from the router. - Put the modules one by one. - Apply the configuration. - The router is stable. The lab test recreated as follows: 1) Disable auto-configuration, that is, "no ccm-manager config". 2) Reload the gateway. 3) Enable the CCM manager configuration and the router does not crash.

Workaround 1: Bypass the start-up configuration and log in via ROMmon without any configuration. Add the configuration one by one. Once the configuration is added, save the configuration and reload the gateway.

Workaround 2: Shut down the router and add the cards one by one in slots 0, 1, 2, 3, and 4. The device is stable until the third slot is inserted and brought up. As soon the router is powered on, after adding the fourth slot, the crash starts. Shut down the router and remove the card in slot 4 (EVM-HD-8FXS/DID). Bring the device up without the card in slot 4 (EVM-HD-8FXS/DID). Remove the "mgcp" and "ccm-manager fallback-mgcp" configuration from the device because the console log is displaying the "Call Manager backhaul registration failed" error message. Shut down the router and add the card which was removed. Bring up the router. Read the ccm-manager fallback-mgcp command and do a "no mgcp/mgcp". The router becomes stable.

Workaround 3: Remove the ccm-manager config command by no ccm-manager config which tears down the connection from the call manager to the MGCP gateway. The gateway will not download the configuration from the call agent at the time of startup. Reload the router. Once the router is back and stable, readd the command.

- CSCub56842

  Symptoms: The router stops passing IPsec traffic after some time.

  Conditions: This symptom is observed when the **show crypto eli** command output shows that during every IPsec P2 rekey, the active IPsec-Session count increases, which does not correlate to the max IPsec counters displayed in the SW.

  Workaround: Reload the router before active sessions reach the max value. To verify, do as follows:

  router#sh cry eli

  ```
  CryptoEngine Onboard VPN details: state = Active
  Capability    : IPPCP, DES, 3DES, AES, GCM, GMAC, IPv6, GDOI, FAILCLOSE, HA
  IPSec-Session :  7855 active,  8000 max, 0 failed
  ```

- CSCub69764

  Symptom: Occasionally, after full chassis reload, all ATM autovc fail to come up upon reception of PADI. CPE gets no PADO. All PPPoEoA sessions fail to establish on the chassis.

  Conditions: Trigger unknown. This condition occurs intermittently, after full chassis reload, once every ~50 reloads.

  Workaround: If the condition occurs, reload the chassis again.

- CSCub74272

  Symptom: Intermittently during Phase II rekey, after new SPIs are negotiated and inserted into SPD, old SPIs are removed and then 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.

- CSCub89144

  Symptoms: In a VTI scenario with HSRP stateless HA, the tunnel state on standby is up/up.

  Conditions: This symptom occurs when HSRP is configured and there is no SSO configuration.

  Workaround: There is no workaround.

- CSCub90459

  Symptoms: If CUBE has midcall reinvite consumption enabled, it also consumes SIP 4XX responses. This behavior can lead to dropped or hung calls.

  Conditions: This symptom occurs when midcall reinvite consumption is enabled.

  Workaround: There is no workaround.

- CSCuc12685

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

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

  Workaround: There is no workaround.

- CSCuc24937

  Symptom: The voice gateway router is configured as a CME for handling ephone reloads due to spurious memory access.

Condition: This symptom occurs as the voice gateway router is capable of handling ephones. Reload is very specific to ephone handling.

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.

- CSCuc40448

  Symptoms: No-way audio is observed on hair-pinned calls back from CUBE to SIP Provider. The call flow is as follows: PSTN caller --Verizon---(sip)---ASR CUBE---(sip)---CUSP---(sip)---Genesis (SIP refer sent to transfer back to Verizon) -- CUSP - CUBE - Verizon -- PSTN

  Conditions: This symptom is observed only after upgrading to Cisco IOS Release 15.2(2)S.

  Workaround: Modify the diversion header on the transfer leg invite. Therefore, the Verizon handles the call differently.

- 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.

- CSCuc54604

  Symptom: CUBE SP does not respond to any SIP messages sent across using TCP. SIP using UDP works fine. Call Flow: Multiple CUCM's ---> SIP --->CUBE SP--->Provider.

Conditions: This defect is noticed on 15.2(01)S01 and is only active when we have calls running SIP TCP. Reason for this behavior is that during the create or close transaction on TCP, the control buffer would be on hold. Therefore, if close of existing TCP connection is needed while the control buffer are all being held, the connection would be marked as dead but not able to notify corresponding peer, therefore the peer might still send data through that connection, which CUBE-SP would think as invalid and get dropped internally.

Workaround: As a workaround we need to send the SIP call as UDP instead of TCP.

- CSCuc56136

  Symptom: Traffic fails to pass on PW.

  Conditions: Configure xconnect on EFP and do RP SSO.

  Workaround: Reconfigure the EFP and xconnect.

- CSCuc65424

  Symptoms: 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, for a dual RP configuration, and when some interfaces are deleted and created again.

  Workaround: Turn off the IDB reuse option.

- 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.

- CSCuc85157

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

  Conditions: This symptom is observed due to the PAT.

  Workaround: There is no workaround.

- CSCuc89800

  Symptom: Receive a **for_us** packet with multiple (thousands of) tunnel headers, make ESP crash.

  Conditions: Router A-------Router B-------Router C there is a tunnel T1 between A and C. In the router A, there is a PBR that makes the packets from B transmitted through T1. In router B there is a default route pointing to A. Then in router A a packet is transmitted through T1 encapsulated with a GRE header. When this packet arriving at router B, due to the flapping of route between B and C, it cannot be sent to C. But it will be sent to A because of the default route. When the packet arriving at A, according to the PBR rule, it will be transmitted through T1 again encapsulated one more GRE header. again and again, this packet will be encapsulated with thousands of GRE header. At last, when the route between B and C no longer flaps, it will arrive at C, and make C crash.

  Workaround: Workaround for customer's scenario: Customer can configure a ACL in router C 's tunnel T1 interface, deny the packet if it has an inner header with the same src addr and dst addr with outer header. But this workaround can't cover the scenario of an attack packet encapsulated with multiple different tunnel headers.

- 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. So in spite of traffic IPsec SA is not coming up leading to packet drops in client network. The same problem is not seen with Cisco IOS Release 15.0(1)M7. This behavior is introduced post-PAL where virtual-interface creates a ruleset where traffic cannot trigger IPsec SA again once IPsec SA is deleted.

Workaround The following are workarounds for this symptom:

- Configure **ip sla** on EZVPN client for split networks, so that IPSec SA will not go down.
- Remove **virtual-interface** from EZVPN client profile if it is not needed.

- CSCuc94687

  Symptoms: SHA2 processing in software causes low throughput or high CPU.

  Conditions: On the Cisco 892 running Cisco IOS Release 15.2(4)M and later, this symptom is observed with SHA2 configured and the onboard crypto engine enabled.

  Workaround: There is no workaround.

- CSCuc95192

  Symptom: The ucode crash is seen.

  Conditions: This symptom occurs when configuring or unconfiguring the static NAT in B2BHA setup.

  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.

- CSCuc98107

  Symptom: The performance of urpf with acl gets downgraded.

  Conditions: The downgrading has been found since 15.3(01)S.

  Workaround: There is no workaround.

- CSCud01502

  Symptom: A crash occurs in CME while accessing a stream in sipSPIDtmfRelaySipNotifyConfigd.

  Conditions: This symptom occurs in CME.

  Workaround: There is no workaround.

- CSCud05368

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

  Conditions: WCCP on ASR1K.

  Workaround: The following are the workarounds for this symptom:

  - Move the deny entries before the permits when possible (especially for deny ... host ...), but it still may not work in some situation.

  - Use different redirect ACLs for each service, and remove the unnecessary ones for specific services.

- CSCud06887

  Symptom: There is no sync of SADB on an active router when it reloads from the current standby router.

  Conditions: This symptom occurs when the active and standby routers are up. Whenever a session is up, there is a sync of SADB from active to standby. When active reloads and is up, there is no sync of SADB from the current active router.

  Workaround: Remove the **isakmp-profile** configuration under the crypto map.

- 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.

- CSCud14033

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

  Conditions: Remove and add uRPF and ACL configuration in the following manner while the traffic is runnin:, **copy remove_config running** and **copy add_config running.**

  Workaround: There is no workaround.

- 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.

- CSCud24885

  Symptom: See some drops: **FirewallInvalidZone 12676.**

  Conditions: ASR with WCCP and ZBF and netflow both configured.

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

- CSCud25675

  Symptoms: Packet drop might be observed during IP Security (IPSec) rekey.

  Conditions: This symptom is observed on a Cisco ASR1000 series router when functioning as an IPSec termination and aggregation router, with Internet Key Exchange.

  Workaround: There is no workaround.

- CSCud35550

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

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

  Workaround: There is no workaround.

- CSCud37568

Symptom: Memory leak in GTP PDP pool.

Conditions: GTP AIC must be configured.

Workaround: There is no workaround.

- CSCud44854

  Symptom: Hash table not memset for ALG during intialization.

  Conditions: 1. Start sip/h323/... traffic. 2. Established NAT session over 60~70K 3. Send CLI combinations with the following actions: A. clear ip nat trans * . B. Shutdown inside/outside traffic interfaces C. Remove nat/alg config D. Reconfig nat/alg and unshut interfaces.

  Workaround: There is no workaround.

- CSCud49494

  Symptom: ESP crashes with multicast service reflect config when recieving UDP fragmented packets.

  Conditions: Multicast service reflect configured udp fragments recieved in the VIF interface.

  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) is: 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 or bursty control packets.

  Workaround: There is no workaround.

- CSCud51791

  Symptom: Memory leak is seen on the router related to CCSIP_SPI_CONTRO.

  Conditions: This symptom is observed in CME SIP phones with Presence in running configuration.

  Workaround: There is no workaround.

- CSCud53401

  Symptom: The router crashes due to a hardware interrupt.

  Conditions: When FRF.12 is configured on ESP100 or 1RUVE2, the recycle queue cannot be changed on-the-fly because there may be packets inflight that will be enqueued to this queue by the hardware.

  Workaround: There is no workaround.

- CSCud57841

  Symptom: When the Ethernet SPA with Catskills SFPs (GLC-SX-MMD /GLC-LH-MMD) is reloaded, the SPA could go out of service with the following error message:

  ```
  %SMC-2-BAD_ID_HW: SIP0/0: Failed Identification Test in 0/0 [7/0]
  ```

  Conditions: This symptom occurs when the Ethernet SPA is booted with the Catskills SFPs(GLC-SX MMD/GLC-LH-MMD). The defect could happen during initialization or reload.

  Workaround: Boot the Ethernet SPA without the Catskills SFPs. Insert the Catskills SFPs after the Ethernet SPA has completely booted.

- CSCud58038

  Symptom: Ucode crash seen with nat tgn mode and CLI operation during traffic.

Conditions: 1. Setup sip/h323 traffic. 2. Shut ->clear ip nat tr * -> unshut. 3. Remove ip nat shut clear ip nat tr *.

Workaround: There is no workaround.

- CSCud61366

  Symptom: FP20 and FP40 cards crash 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 to prevent this crash. You may not run into this problem again after FP reboot.

- CSCud63381

  Symptom: Switching from periodic to on-demand DPDs may cause the DPDs to fail intermittently and thus IPSEC Failover may not work correctly.

  Conditions: 1. 7200-VSA 2. IOS 15.1(4)M2. 3. On-demand DPDs configured for IPSEC FO.

  Workaround: Disable the SCTP session: ipc zone default association 1 shutdown.

- CSCud64870

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

  Conditions: The crash happens when there are 5 CDPs for the hub router to fetch CRL. Given that there are multiple CDPs, the hub router fetches CRL in a parallel way, which then lead to a crash under a timing issue.

  Workaround: Setting up only 1 CDP instead of multiple CDPs will avoid the timing condition which leads to the crash.

- CSCud66316

  Symptom: Log messages for REJECT Create-session-response are not printed in sys-log.

  Conditions: GTP AIC should be configured in the UUT.

  Workaround: There is no workaround.

- CSCud66955

  Symptom: SPA-2CHT3-CE-ATM is flapping with Nortel Passport due to very fast bouncing down/up 10s after the interface is brought up.

  Conditions: This symptom is observed in the E3 and DS3 mode.

  Workaround: There is no workaround.

- CSCud67779

  Symptom: One-way audio is observed when a call goes through BACD and comes over SIP trunk.

  Conditions: This symptom occurs when a call comes through SIP trunk and is connected to an agent phone via BACD during the third call xfer, along with the "headset auto-answer" configuration in the ephone.

  Workaround: Remove the "headset auto-answer" configuration in the ephone configuration.

- CSCud71253

  Symptom: Outbound traffic does not flow.

  Conditions: When configuring IPv4 VRF aware ipsec with crypto maps with ivrf=ivrf1 and fvrf=global.

Workaround: Put a route in the global routing table (fvrf) for the network in ivrf pointing the next-hop to the ivrf interface.

- CSCud72509

  Symptom: ESP100 crashed.

  Conditions: NAT configured, TCP segments size 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 "no ip nat service dns tcp."

- CSCud73600

  Symptom: FP crash.

  Conditions: QoS is confgiured on physical interface which is bind to a BDI interface. Stile is configured on the same BDI interface.

  Workaround: There is no workaround.

- CSCud75692

  Symptom: Tunnel QoS is broken.

  Conditions: Tunnel target interface is ATM sub-interface.

  Workaround: There is no workaround.

- CSCud75856

  Symptom: Presence of FP core file.

  Conditions: Under certain very rare (unreproducible in lab) conditions, multicast LRE code can run out of rbufs while serially processing packets, presumably because of the feature chain executed.

  Workaround: Disabling MLRE through configuration command "platform multicast lre off" can be done if condition occurs.

- CSCud86039

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

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

  Workaround: There is no workaround.

- CSCud86240

  Symptom: The Cisco ASR 1000 ESP crashes (ucode core file created) when compressed packets are sent on a Multilink PPP interface using the Cisco IOS XE 3.5 Release and earlier Cisco ASR 1000 software images. On Cisco IOS XE 3.6 Release and later on Cisco ASR 1000 software images a crash does not occur, but routed traffic on configured interfaces are not forwarded. However, local traffic between the peer routers may still 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: This symptom is observed 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 Cisco IOS XE 3.5 Release and an earlier Cisco ASR 1000 software image.

  Workaround: Remove the compress [mppc | stac | predictor] feature configuration from all interfaces as this functionality is not supported on the Cisco ASR 1000 router. The software fix associated with this bug report will be removing this configuration option from the Cisco ASR 1000 router.

- 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.

- CSCud88517

  Symptom: System may be out of service.

  Conditions: This symptom is observed on a Cisco ASR1000 series router when 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 could crash due to a NAT bind age timing.
  Conditions: This is a rare timing condition which was triggered by the RG infra toggle .
  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.

  Condition: This symptom occurs under the following conditions: -using an ACL for both IPv4 and IPv6 in a policy-map -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 can not be configed less then 16. If so, the number of learned prefix will be much lesser then it should be.

  Conditions: When PfR is enabled.

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

- 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.

- CSCue15619

  Symptom: SBC CLI hung.

  Conditions: Configure signaling-peer-port when the adj is attached, new vty terminal would be hung.

  Workaround: There is no workaround.

- CSCue25321

  Symptom: BFD flaps continuously upon ESP switchover.

  Conditions: 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.

- CSCue39206

  Symptom: ES crashes after the second 401 challenge.

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

  Workaround: There is no workaround.

- CSCue44651

  Symptom: On a Cisco ASR1000 series router with GTP ZBFW enabled, pinholes are opened on GTP-U for the initiating side. TRaffic back is dropped since the UDP-SRC port of the initiation side is changed from xxxx to 2152.

  Conditions: This symptom is observed when GTP ZBFW is enabled.

  Workaround: There is no workaround.

- 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.

- CSCue47484

  Symptom: BFD neighbour is not up.

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

  Workaround: There is no workaround.

- CSCue55762

  Symptom: x86-based platforms can crash after ~27x days.

  Conditions: This symptom is observed with x86-based platforms. Most likely, this issue is not seen on RP1, 1RU, and 2KP as their CPU feature set does not have both constant_tsc and nonstop_tsc on.

  Workaround: Reboot the box. In any case, plan to upgrade to a release which has the fix within 7 months (the first release that has the fix is Cisco IOS XE Release 3.7.3S.)

- 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.

- CSCue63756

  Symptom: FPMAN-RP memory increases when the uut flaps the interface facing the CE side.

  Conditions: 8K l2tpv3 scaling event monitor.

  Workaround: There is no workaround.

- CSCue69527

  Symptom: More than 95 SCCP controlled FXS ports cannot be configured on the Cisco VG350. The debug output for "debug ccm-manager config-download errors" is as follows: cmapp_sccp_gw_start_element_handler: warning - max number of interfaces reached.

  Conditions: This symptom occurs when configuring more than 95 SCCP FXS ports on the Cisco VG350 using CUCM.

  Workaround: There is no workaround.

- 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.

- CSCue85737

  Symptom: ASR with PKI certificate may crash when issuing 'show crypto pki certificate'.

  Conditions: Issue 'show crypto pki certificate' on ASR with pki certificate.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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 3.7.2T

This chapter contains the following sections:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.2T

This section documents resolved issues on Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.2T.

- CSCuc97477

  Symptom: A new feature has been introduced for dummy packet support.

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCud39590

  Symptom: A new feature has been introduced for dummy packet support.

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCud54133

  Symptom: During the FIPS code review, a non-conformance was found. Specifically, when the SP 800-90 Deterministic Random Bit Generator (DRBG) calls the ACT chip for a seed, there is no Continuous Random Number Generator Test applied to the value output from the chip.

  Conditions: The symptom is observed when the SP 800-90 DRBG calls the ACT chip for a seed, there is no Continuous Random Number Generator Test applied to the value output from the chip.

  Workaround: There is no workaround.

- CSCud80859

  Symptom: IPSec dummy packet support is currently not available in the Cisco IOS XE 3.7 image. (This is the DDTS used to add the support in Cisco IOS XE Releases 3.7 and 3.7.2T).

  Conditions: This symptom is observed at all times.

Workaround: There is no workaround.

- CSCud88517

  Symptom: The system may be out of service.

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

- CSCue26378

  Symptom: On a Cisco ASR 1000 Series Router, IPSec dummy packet counter is only shown in the PD specific CLI under the **show pl ha qfp act feat ipsec sa ##** command. It is not shown under the **show crypto ipsec sa det** command as dummy packets send or receive.

  Conditions: This symptom is observed when you issue the **show crypto ipsec sa det** command.

  Workaround: There is no workaround.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.2S

This chapter contains the following sections:

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.2S

This section documents the unexpected behavior that might be seen in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.2S.

- 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.

- CSCty24937

  Symptom: TCAM exhaustion and FP crash with IDFW scale > 300 class-maps on 2ru or RP1/RP10 box.

  Conditions: TCAM exhaustion and FP crash with IDFW scale > 300 class-maps on 2ru or rp1/rp10 box.

  Workaround: There is no workaround.

- CSCua30168

  Symptom: IOSd restart in 4k mixed tunnel scaling test.

Conditions: This symptom is observed during mixed tunnel scaling test and high traffic.

Workaround: There is no workaround.

- CSCua59573

  Symptom: An issue is seen after running certain functionality tests of VPLS.

  Conditions: The issue is seen in VPLS scaled test bed after running certain functionality tests. The issue is reproducible on running the script.

  Workaround: The issue is not reproducible manually.

- CSCub69764

  Symptom: Occasionally, after a full chassis reload, all ATM autovc fail to come up after reception of PADI. CPE gets no PADO. All PPPoEoA sessions fail to establish on the chassis.

  Conditions: Trigger unknown. This is occurring intermittently, after full chassis reload, once every ~50 reloads.

  Workaround: If the condition occurs, reload the chassis.

- CSCuc55907

  Symptom: Under certain circumstances, an Aggregation Services Router 1000 with a single Embedded Service Processor 40 (ESP40) and dual Router Processor 2 cards (RP2), will reload if the ESP40 is replaced.

  Conditions: When running an ASR1000 with dual RP2 running is SSO mode and a single FP40, if the FP40 is removed/replaced, the entire router will reload and leave a core file behind. The router is working as an L2TP access concentrator with thousands of active tunnels and passing traffic, but other situations my trigger the same reaction.

  Workaround: Running with redundant FP40 may help alleviate the situation.

- CSCuc65424

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

  Conditions: This symptom is observed when **db reuse** is turned on, on a dual RP configuration. Some interfaces are deleted and recreated.

  Workaround: Turn off the **idb reuse** option.

- CSCuc85157

  Symptom: Packet is dropped with reason of NatIn2out.

  Conditions: PAT

  Workaround: There is no workaround.

- CSCuc89800

  Symptom: Configured IP GRE tunnel causes ESP to crash.

  Conditions: A packet containing multiple IP/GRE headers being similar causes ESP to crash.

  Workaround: Configure ACL to block the traffic.

- CSCuc90992

  Symptom: in a scale situation with several DENY statements and several NAT pools, the following configuration hit the deny-jump. TCAM limitation and NAT does not work.

  ```
  Oct 16 16:27:33.835 MEST: %CPP_FM-3-CPP_FM_TCAM_ERROR: F0: cpp_sp:  TCAM limit
  exceeded: Class group nat-class:1001.1 could not be successfully edited. Please remove
  the class group from the interface.
  ```

Conditions: NAT and SIP NAT ALG are required. For SIP NAT ALG, not all embedded IP addresses within SIP payload need to be translated. For this reason, aa exceptions need to be defined.

```
ip nat pool <name>-hosts 10.200.0.36 10.200.3.253 netmask 255.255.252.0 ip nat inside source list all-nat pool <name>-hosts vrf <name> ! ip access-list extended all-nat deny ip 192.168.152.0 0.0.1.255 192.168.152.0 0.0.1.255  permit ip any 192.168.152.0 0.0.1.255.
```

Workaround: There is no workaround.

- CSCud05368

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

  Conditions: WCCP on ASR1K.

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

- CSCud24885

  Symptom: Some packet drops seen: `FirewallInvalidZone 12 676`

  Conditions: Netflow configured at the same time.

  Workaround: Ping the destination on ASR1K before introducing WCCP traffic.

- CSCud25675

  Symptom: Packet drop may be observed during IP Security (IPSec) re-key.

  Condition: This symptom is observed on a Cisco ASR1000 series router when I14 is configured.

  Workaround: There is no workaround.

- CSCud30472

  Symptom: IOSd crashes at `ace_polo_list_cm_head_nodes`.

  Conditions: This symptom is observed while entering the **show crypto ace polo detail** command after configuring 192-bit AES key for IPv6 OSPF encryption.

  Workaround: There is no workaround.

- CSCud33184

  Symptom: ESP ucode crash is seen on the ASR causing loss of traffic forwarding.

  Conditions: CGN NAT is enabled on the router.

  Workaround: There is no workaround.

- CSCud35735

  Symptom: Ucode along with fman_fp core seen in UUT with GTP_AIC_FUNC_POLICY_CHANGE.

  Conditions: This symptom is observed while sending traffic from SGSN

  Workaround: There is no workaround.

- CSCud36113

  Symptom: Ping fails between CE routers.

  Conditions: Configure MPLS VPN Inter-AS IPv4 BGP Label Distribution and flaps **mpls bgp forwarding** in the interface between ASBRs

  Workaround: There is no workaround.

- CSCud36156

  Symptom: RP switchover due to a kernel crash.

  Conditions: Dual RP running on ASR with 15.1(3)S1.

  Workaround: There is no workaround.

- CSCud37921

  Symptom: Update PDP context requests are dropped if GSN address is not identical with GSN address provided in Create PDP context request.

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

  Workaround: There is no workaround.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.2S

This section documents resolved issues on Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.2S.

- CSCsu57181

  Symptom: When the retransmission number is changed, the next rekey does not reflect this change.

  Conditions: Change number of retransmissions from 2 to 5, and the number stayed at 2; and when changing the retransmissions from 2 to 1, the number of retransmissions stayed at 2. This happen for both unicast and multicast rekey.

  Workaround: Clear crypto gdoi and start over again.

- CSCts52120

  Symptoms: Tracebacks are seen for PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT.

  Conditions: This symptom is observed with RPSO.

  Workaround: There is no workaround.

- CSCtv01521

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

  Conditions: 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 32bytes of the packets causing this. Or use the debug ip cef packet all input rate 10 dump command to dump the full packets.

- CSCtx71747

  Symptom: CPP Ucode crash on ASR1000-ESP40.

  Conditions: This has been seen on ASR1006 (RP2) running asr1000rp2-advipservicesk9.03.02.02.S.151-1.S2.bin. It will impact any systems that use MLRE (FP40, FP80, and so on).

  Workaround: Use the **set platform hardware qfp act feature multicast v4mcast lre off*** command or for permanent setting used configuration command: **conf> platform multicast lre [on | off]**. *This is a temporary solution until the software bug is fixed.

- CSCtz38010

  Symptom: Platform max numbers for ASR1k NAT44 and NAT64 is not set for KP and FP80.

  Conditions: Scalability numbers are not correct.

  Workaround: There is no workaround.

- CSCtz69527

  Symptom: Route not found on UUT for RRI test cases.

  Conditions: When the testcase for RRI, reverse-route remote-peer 16.0.0.1 gateway is checked, route is not found on the router.

  Workaround: There is no workaround.

- CSCtz94286

  Symptom: IOS router with enabled ISM-VPN-29 module does not process ESP traffic when GRE packets are denied on the outside ACL.

  Conditions: There are 2 conditions that must BOTH be met to experience this issue: 1. The router uses an ISM-VPN module, and the module is installed and enabled. 2. There is an ACL on the 'outside' interface of the router that does not permit GRE traffic from the remote IPSec peer.

  Workaround: There are 2 work-arounds for this issue: 1. Permit GRE traffic from the remote IPSec peer or 2. Disable the ISM-VPN module.

- CSCua45206

  Symptom: Hub router crashes while removing Stale Cache entry.

  Conditions: Crash occurs when 2 spokes are translated to same NAT address.

  Workaround: Spokes behind the same NAT box must be translated to different post-NAT Addresses.

- CSCua54514

  Symptom: bqs queue output is different for FP10 and FP80.

  Conditions: Output difference is seen while checking the **sh plat hard qfp ac fe qos queue out all d** output.

  Workaround: There is no workaround.

- CSCua55423

  Symptom: security-association lifetime not reflected in configs and script was expected the lifetime 120 to be reflected while checking for output.

  Conditions: security-association lifetime 120 was not reflected in sh run putout.

  Workaround: DT need to fix the issue.

- CSCua81565

  Symptom: ASR1K/RP2/ESP40 on 15.1(3)S3 acting as L2TP BRAS.

  Conditions: Periodically the ESP F0/F1 crashes with the reason: `%CPPHA-3-FAULT: F0: cpp_ha: CPP:0 desc:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR(interrupt) class:OTHER sev:FATAL id:2121 cppstate:RUNNING res:UNKNOWN  flags:0x7 cdmflags:0x0.`

  Workaround: There is no workaround.

- CSCua82440

  Symptoms: FNF records do not get exported when a user reloads the router.

Conditions: This symptom occurs if a user configures a non-default export-protocol, that is, anything other than "netflow-v9". If the user configures a non-default export-protocol such as IPFIX or netflow-v5, after saving the configuration to the start-up configuration and reloading the router, the exporter will not export any records.

Workaround: Either one of the following methods will fix this issue: 1. Remove and reconfigure the exporter configuration after reload. 2. Change the export-protocol to the default value (netflow-v9).

- CSCua87896

  Symptom: qfp exmem is exhausted in the standby fp

  Conditions: TCP is used for Sip signalling.

  Workaround: There is no workaround.

- CSCua91473

  Symptoms: Memory leak occurs during rekey on the IPsec key engine process.

  Conditions: This symptom occurs after rekey, when the IPsec key engine does not release KMI memory, causing the IPsec key engine holding memory to keep increasing.

  Workaround: Clear crypto session for IPsec key engine to release memory.

- CSCua94563

  Symptom: Traceroute may return * * * instead of host.

  Conditions: When going v4->v6 through NAT64 stateful on ASR1k.

  Workaround: There is no workaround.

- CSCub05559

  Symptom: on 1ru, after system booted rarely the bootflash (eUSB) gets disconnected. as a result, the system will reboot as the system cannot stay up without eUSB storage.

  Conditions: This can occurs randomly (no specific pattern, but usually after 2~3 days). so this is a big issue for system stability.

  Workaround: There is no workaround.

- CSCub13983

  Symptom: There are 2 calls to mcp-sysinit.

  Conditions: This issue is observed all the time.

  Workaround: There is no workaround.

- CSCub19408

  Symptom: Router may no longer be accessed through the console port. Power cycle is required to recover.

  Conditions: Console loss occurs randomly when console port is used to enter router configuration.

  Workaround: There is no workaround.

- CSCub58775

  Symptom: An ASR1000-system might see a crash of the stby-RP.

  Conditions: This could be seen after an OIR of a power-supply and perhaps similar events.

  Workaround: There is no workaround.

- CSCub65151

  Symptom: ASR1K CPP crashes when shutting down core facing MPLS intf on NPE.

Conditions: Happens rarely.

Workaround: There is no workaround.

- CSCub68021

  Symptom: A "show interface" on a SPA interface shows "0" for "unknown protocol drops", yet when the same interface is polled for ifInUnknownProtocols, a value is returned.

  Conditions: Normal polling.

  Workaround: There is no workaround.

- CSCub69414

  Symptom: Traceback at FreeUInt64 on booting up router.

  Conditions: This symptom is observed on an ASR1006 running mcp_dev towards XE38. On booting up the router a traceback is seen.

  Workaround: Tracebacks are seen because of snmp-server enable traps entity-qfp mem-res-thresh. Disable the snmp-server enable traps entity-qfp mem-res-thresh.

- CSCub73484

  Symptom: Standby ESP100 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.

- CSCub76612

  Symptom: the console reports "%FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image: PFR TT Enable download to CPP failed" and prints traceback. also, ASR may reload with fman_fp core file.

  Conditions: FMAN-FP reports PfR ERR log when there is PfR session flapping between MC and BR.

  Workaround: There is no workaround.

- CSCub82275

  Symptom: An ASR 1K may experience reloads on the ESP module due to a CPP driver fault during an in-2-out NAT translation. Issue has been seen with IOS 15.2S, but not in 15.1S.

  Conditions: NAT enabled. No other requirements known.

  Workaround: Disable NAT or downgrade to a 15.1 release.

- CSCub85608

  Symptom: ASRNAT address leak may occur. This will show a larger number of allocated addresses in 'sh ip nat stat', then the translations that exist for that address through 'sh ip nat trans'.

  Conditions: This issue only occurs when a dynamic route-map configuration is used and the NAT sub-drop code ESP_CREATE_FAIL is incrementing (there must be ESP traffic).

  Workaround: The leaked addresses can be reclaimed periodically by executing a 'clear ip nat trans *', but that will be disruptive to users so it should be scheduled for off-hours.

- CSCub89150

  Symptom: Pw with backup.

  Conditions: Switch between active/standby pw.

  Workaround: Reload the routers.

- CSCub89157

  Symptom: Message is dropped.

  Conditions: This symptom is observed when cause is not equal to 128.

  Workaround: Resend the message.

- CSCub89711

  Symptom: Atm keyword for the show command disappears.

  Conditions: Perform a powered shutdown of the SPA card and bring it back up using no form of the previous command.

  Workaround: There is no workaround.

- CSCub91178

  Symptom: ALG FTP44 doesn't work, and the data path fails to establish.

  Conditions: Divide two networks into two vrf, both client and server reside in different network.

  ```
  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's 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's one inside static nat ip nat inside
  source static 192.168.0.2 202.119.0.2 vrf vrf_out     Client runs FTP,active mode.
  ```

  Workaround: Use dynamic NAT instead.

- CSCub95141

  Symptoms: FP Pending Refs are observed when "cypto map <> local-address loopbackX" is removed from the configuration when the crypto map is applied on a subinterface.

  Conditions: This symptom is observed with the following configuration: `crypto map cry local-address Loopback0 interface GigabitEthernet0/0/0.100 crypto map cry interface GigabitEthernet0/0/0.200   crypto map cry.`

  Workaround: Remove "crypto map" from the subinterface first and then remove "crypto map <> local-address loopbackX."

- CSCub97641

  Symptom: When netflow test is performed on NAT cgn mode, an abnormal netflow log was found. This issue is not observed in the default mode.

  Conditions: Config as cgn 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.

- 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: Turn on permit-error.

  Workaround: There is no workaround.

- CSCuc02916

  Symptom: IPv6 packet with Hop-By-Hop extension header is dropped when the packet is sent out to L2TP Virtual-Access interface.

  Condition: ASR is configured as L2TP LNS. At that time, EssUnsupPktType drop counter is incremented.

Workaround: There is no workaround.

- CSCuc04837

  Symptom: On serial interface the IOS counters for input packets, input errors and aborts increase even after the interface is administratively shutdown.

  Conditions: No specific condition.

  Workaround: As this is a corner case situation, un-shutting and shutting down the interface may resolve the issue.

- CSCuc05671

  Symptom: The console reports "[aom]: (ERR): Unable to find async context for AOM" and traceback.

  Conditions: FMAN-FP reports PfR ERR log when there is PfR session flapping between MC and 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: If you copy the policy to a set number that didn't previously exist, this problem does not occur; it only seems to happen if you reuse a number that was removed previously.

  Workaround: Copy to new set number which has not been used before.

- CSCuc11853

  Symptoms: T1 controller will stay DOWN after switchover.

  Conditions: This symptom is seen when SATOP is configured on T1.

  Workaround: Perform a shut and no shut.

- CSCuc16716

  Symptom: This is not a defect but an enhancement, so there are no symptoms.

  Conditions: This is an enhancement, so there are no conditions.

  Workaround: It is not an defect but only and enhancement.

- CSCuc25529

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

  Conditions: This has been observed on an ASR1k and 7200 running IOS 15.2(4)S and 15.1(4)M.

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

- CSCuc26232

  Symptom: Reload indicating "stuck thread" may occur.

  Conditions: On clear ip nat translations vrf <vrf-name> *

  Workaround: Use clear ip nat trans * This issue exists only on XE3.7.1.

- CSCuc31692

  Symptom: ASR1K ucode crash with scaled MLPPP configuration with sustained high data rates across most bundles.

Conditions: Highly scaled MLPPP configuration with sustained high data rates across most bundles. Problem has only been seen with ESP40. instances of encountering this issue are small as this issue has only been seen in a lab environment under extremely high data rate conditions.

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. Note that 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 (that is, 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 through the **clear ppp interface <*Bundle-Virtual-Access-intf-name*>** command.

- CSCuc34574

  Symptoms: A pending-issue-update is seen at SSL CPP CERT on the Cisco ASR 1002, ESP-1000 platform.

  Conditions: This symptom is observed with the following configuration: `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.

- CSCuc40585

  Symptom: Ucode crashes when gtp aic inspect packets.

  Conditions: GTP aic configured.

  Workaround: There is no workaround.

- CSCuc42083

  Symptom: fman_fp Core file seen.

  Conditions: Config GreoIPsec with tunnel protection and configure more than 1k route-maps.

  Workaround: There is no Workaround.

- CSCuc44071

  Symptom: GRE keep-alives are going 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 keep-alives 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 keep-alives will be encrypted as long as there is no CEF adjacency on the Tunnel interface when in protocol down state (that is, no output from **show adjacency tunnel <number> detail**).

- CSCuc45528

Symptoms: Incremental leaks are seen at :__be_nhrp_recv_error_indication.

Conditions: This symptom occurs when the NHRP error indication is received on the box. This issue is seen only if CSCub93048 is already present in the image. CSCub93048 is available from Cisco IOS Release 15.3M&T onwards.

Workaround: There is no workaround.

- CSCuc47399

  Symptoms: IKEv2 STOP Accounting records show wrong counters for packets/octets, when the sessions are locally cleared using **clear crypto sa** or **clear crypto session**.

  Conditions: This symptom is observed with latest Cisco IOS XE Release 3.8S images when IKEV2-Accouting is enabled. This issue is easily reproducible with a single session, and may be service impacting as STOP Accounting records are usually used for billing purposes.

  Workaround: The STOP records reflect the right counters when the disconnect is through the remote-end.

- CSCuc57822

  Symptom: NBAR classification granularity reduced for some protocols or some protocols may be classified as unknown.

  Conditions: The following command can be used to clearly know if this is the bug at hand: **test platform hardware qfp active feature nbar function sui_gmc_show_chunks_brief**. If the "errors?" column has a non zero value, it is likely caused by the problem described here.

  Workaround: Restarting NBAR will typically solve the problem. If a protocol pack is loaded, a simple way to restart NBAR would be to unload and reload the protocol pack. In order to workaround the problem and verify that the problem is resolved, use the following steps: 1. Clear the above counters using the command: **test platform hardware qfp active feature nbar function sui_gmc_reset_counters** 2. Verify that the number of errors has been cleared: **test platform hardware qfp active feature nbar function sui_gmc_show_chunks_brief** 3. Enter configure mode: **config terminal** 4. Unload the protocol pack: **no ip nbar protocol-pack** <*protocol-pack-filename*> 5. Re-load the protocol pack: **ip nbar protocol-pack** <*protocol-pack-filename*> 6. Verify the number of errors is 0: **test platform hardware qfp active feature nbar function sui_gmc_show_chunks_brief**.

- CSCuc58513

  Symptom: Fp reload.

  Conditions: ALG traffic with ACL limit configuration.

  Workaround: Remove ACL limit configuration with ALG traffic.

- CSCuc60435

  Symptom: Packets with single digit MNC are not matched in L7 class-map. Instead counters are increasing in class `class-default 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: Match criteria in 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.

- CSCuc65609

Symptom: During SIP attack, NAT causes ESP lock-up.

Conditions: SIP registration attack.

Workaround: Use ACL to block SIP attack.

- CSCuc67468

  Symptom: **sh plat h q a f nat data dynbin** output gets into a loop.

  Conditions: When executed on ASR1K.

  Workaround: Use **sh ip nat trans** and its filters for showing this information.

- CSCuc71706

  Symptoms: Execution of the **show run** command and other commands such as **copy run start** and **show access-list** cause the router to stop for a few minutes before completing.

  Conditions: This symptom is observed with Cisco ISR G2 routers. This issue is seen only with IPV6 configured and used.

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

- CSCuc75142

  Symptom: ucode crash when h323 alg traffic passed through router.

  Conditions: Seen with alg traffic.

  Workaround: Remove hsl logging.

- CSCuc76670

  Symptoms: 2X1GE-SYNCE (metronome) SPA does not boot on a 2RU (Cisco ASR 1002).

  Conditions: This symptom is observed with Cisco IOS XE Release 3.7S onwards, when metronome SPA (2X1GE-SYNCE) fails to boot on a 2RU. An error message indicating that the SPA is not supported is displayed on the RP console.

  Workaround: There is no workaround.

- CSCuc77704

  Symptoms: 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.

- CSCuc78320

  Symptom: QFP crashes with icmpv4 error packets when ZBF debugs are enabled (**debug platform hardware qfp active feature firewall datapath global all detail**)

  Conditions: This condition is observed when ZBF debugs are enabled.

  Workaround: Don't enable ZBF debugs with "detail" or "drop" keywords for all traffic. Instead enable ZBF debugs only for the traffic you'd like to debug. See CSCtf45361 to see how to do it.

- CSCuc78499

  Symptom: GTPv1 memory chunk leak.

  Conditions: GTP AIC is configured.

  Workaround: There is no workaround.

- CSCuc81993

  Symptom: Need ikev2 framed route support on server.

  Conditions: Need ikev2 framed route support on server.

  Workaround: There is no workaround.

- CSCuc93053

  Symptom: WCCP stops working after adding ZBF. We see 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.

- CSCud01905

  Symptom: Match not apn is not working.

  Conditions: Basic gtp message flow.

  Workaround: There is no workaround.

- CSCud03877

  Symptom: After volume rekey, ipsec pd flow set both hard and soft limit of traffic limit to 0.

  Conditions: Volume rekey set to 0.

  Workaround: Clear crypto session recover volume rekey value.

- CSCud16127

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

  Conditions: IMSI is invalid.

  Workaround: There is no workaround.

- CSCud16274

  Symptom: Cpp crash with core dump file and traceback.

  Conditions: Session setup rate is 10.

  Workaround: There is no workaround.

- CSCud21773

  Symptom: DHCP reply message was dropped in dataplane after RPSO or clear ipv6 neighbor.

Conditions: 1. Setup DHCPv6 binding. 2. Clear ipv6 neighbor/ RPSO and without traffic before adjacency convergence. The dhcp reply message is dropped in the dataplane.

Workaround: There are several workarounds: 1. Send downstream traffic to client which will relearn the neighbor. 2. Clear ipv6 route X::X/prefix <dhcp installing route> to relearn the neighbor. 3. Client can reconnect after the dhcp session timeout.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.1S

This section describes the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7S. It contains the following topics:

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.1S

This section documents the unexpected behavior that might be seen in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.1S.

- CSCtt01529

  Symptom: A %SPA_CHOCX-3-FATAL_ERROR occurs on hard online removal of SPA-1XCHSTM1-OC3 when controller of the SPA is configured as net-sync clock source on the Cisco ASR1002-X router.

  Conditions: This issue occurs when controller of SPA-1XCHSTM1-OC3 is configured as the active network-clock input source.

  Workaround: Avoid hard removal of the SPA when SPA-1XCHSTM1-OC3 is selected as the current active clock input. However, insterting the SPA in the same subslot after the occurrence of this error does not affect the netsync capability. Therefore, the error while SPA removal can be neglected.

- CSCtt11188

  Symptom: The BITS IN clock with RP switchover stays locked even with Alarms On link on ASR1002-X.

  Conditions: When BITS IN is active clock source for the system and RP switchover occurs, the BITS IN with Active Alarms ON, is seen as active clock source.

  Workaround: There is no workaround.

- CSCuc54129

  Symptom: The **request platform software package install rp 0 snapshot to harddisk** command saves subpackages to bootflash instead of hard disk.

  Conditions: This issue is seen only on the ASR1002-X router.

  Workaround: Use the bootflash instead for this option.

- CSCuc15992

Symptom: Multiple cpp_cdm tracebacks occur while CPP microcode is being collected in a crash dump file.

Conditions: These tracebacks occur while collecting a CPP microcode is being collected in a crash dump file.

Workaround: There is no workaround. However, the cpp_cdm tracebacks do not have any impact on the working of the router and can be ignored.

- CSCtz08687

  Symptom: When the command **show platform hardware qfp active datapath utilization**, is execute on CSR1000v platform, te output always shows the Processing: Load (pct) as 100%.

  Conditions: This issue occurs when **show platform hardware qfp active datapath utilization** is executed.

  Workaround: Use the **show platform so status control-processor bri** command. CPU 2 and CPU 3 form the data plane. For example:

```
VXE-21#sh pl so status control-processor bri
Load Average
 Slot  Status  1-Min  5-Min 15-Min
  RP0 Healthy   1.15   0.59   0.44

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  3988596  2675940 (67%)  1312656 (33%)   2504260 (63%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0   0.50   2.30   0.00   2.00  17.90  77.30   0.00
         1   0.50   0.70   0.00  98.79   0.00   0.00   0.00
         2  22.50   7.10   0.00   0.00   0.00   0.40   0.00
         3  23.30  21.20   0.00  25.30   0.00  30.20   0.00
```

- CSCtw74124

  Symptom: For a slot housing the Cisco ASR1000-SIP40, or on a Cisco ASR1002-X, the output of the **show platform hardware slot <slot#> plim buffer settings detail** command always shows the value of Max always as “0“ in the "Fill Status Curr/Max" filed, even when the Rx buffers have been utilized.

  Conditions: When the SPA Aggregation ASIC has been flow controlled by the Network Processing Unit, the buffers inside the SPA Aggregation ASIC will start filling up.

  Workaround: There is no workaround.

- CSCtx89616

  Symptom: The BITS output network clock configuration sends an invalid QL value when it is configured for the first time on a back-to-back Cisco ASR1002-x setup.

  Conditions: This issue is observed after the router reloads with configuration of the BITS e1 output network clock source. The reloaded router sends QL-INV to the remote end.

  Workaround: Reconfigure BITS e1 output network clock source.

- CSCty21018

  Symptom: Network boots from ROMMON may occasionally run very slowly. Sometimes, booting from a "tftp:" device may appear to stall or run very slowly.

  Conditions: This issue occurs when a user attempts to boot from a "tftp:" device.

Workaround: In nonautoboot situations where the console port is connected, and under user supervision, perform a reset.

If the system is configured to auto boot, reconfigure the TFTP_TIMEOUT environment variable from its present value to a value longer than the expected boot time, considering the network and server load. If the system finds itself in this slow-booting mode while auto booting, the transfer will time out, and autoboot will reset and attempt to net boot the file again.

A value of 300 seconds can be chosen as a suggested starting value. From the ROMMON prompt run:

```
TFTP_TIMEOUT=300
sync
```

Note This caveat pertains to the 15.2(4r)S1 ROMMON release.

- CSCty49537

  Symptom: When IPX traffic is introduced at 150 KPPS and the punt policer is changed from 40KPPS to the highest limit, which is 146 KPPS, lsmpi-rx consumes more CPU resources and tail drops occur.

  Conditions: This issue occurs when punt traffic is introduced at high rates while the punt policer is modified from the default setting.

  Workaround: Do not maintain a high punt packet traffic rate.

- CSCtz64939

  Symptom: Cisco ASR1000 RP2 and Cisco ASR1001 may report the following message:

  ```
  %IOSXEBOOT-1-BOOTFLASH_FAILED_MISSING: (rp/0): Required Bootflash disk failed or
  missing, reloading system.
  ```

  The reload of the system recovers the device. There is no loss of data due to the device disconnect. In a redundant hardware configuration, there is no loss of service, and the standby takes control when the active system reloads. In a dual IOSd configuration, the platform reloads fully. If the eUSB is inaccessible during boot, an additional reload may occur, resulting in a longer-than-expected boot time.

  Conditions: This error may occur when an embedded eUSB device is a part of the configuration.

  Workaround: There is no workaround to avoid the disconnect of the boot flash device. Since the boot flash device is monitored as a critical device for correct system operation, it is necessary to reload the system to reset and recover the device.

- CSCua10477

  Symptom: The Cisco ASR1002-X router with large numbers of MLPPP bundles may experience a crash preceded by the following message, followed by a traceback and eventual reload of the router:

  ```
  %CPPOSLIB-3-ERROR_NOTIFY: SIP0: cpp_cp:  cpp_cp encountered an error
  ```

  Conditions: This issue occurs on Cisco ASR1002-X router with large numbers of MLPPP bundles.

  Workaround: Keep the number of single-link MLPPP bundles under 4000, and the total number of multimember MLPPP bundles under 2000.

- CSCua20029

  Symptom: The **show platform hardware qfp active feature epc client statistics 0** command does not respond.

Conditions: This issues occurs while using command in multi terminal.

Workaround: Use one terminal.

- CSCua82440

  Symptom: FNF records do not get exported.

  Conditions: The Cisco ASR 1002-X router boots with preconfigured FNF exporter when export protocol is IPFIX and the platform is RP1 or ASR1002-X.

  Workaround: Reconfigure exporter.

- CSCub09099

  Symptom: When BGP MDT address-family is configured with one or more VRF having mdt default x.x.x.x with 4000 VRF, out of which 400 VRF have "mdt default x.x.x.x" and with 8000 BGP neighbors in VRF (4K IPv4 & 4K IPv6), then router takes approximately 30 minutes to apply the configuration.

  Conditions: This issue occurs if configured neighbors are under BGP VRF address-family with update-source command, that is **neighbor X.X.X.X update-source *interface***.

  Workaround: Do not use **neighbor X.X.X.X update-source *interface*** under BGP VRF address-family.

- CSCub17584

  Symptom: IOSD crashes occur with 1000 MVPN sessions. When the sessions are cleared, all the IGMP joins are released, then the sessions are brought up. When about 400 to 500 IGMP sessions join, a crash is screen.

  Conditions: This issue occurs when you clear 1000 MVPN sessions on LAC using the command **clear pppoe**.

  Workaround: There is no workaround.

- CSCub24053

  Symptom: The BPS and PPS information shown in the output of **show platform hard qfp active data utilization** is inaccurate for ASR1002-X and ESP100.

  Conditions: There are no specific conditions under which this symptom occurs.

  Workaround: There is no workaround.

- CSCub38910

  Symptom: COOP failure messages are seen continuously on a standby RP. However, there is no impact on the functionality of the standby RP. This is an erroneous messaging issue.

  Conditions: This issue is seen on a HA setup.

  Workaround: There is no workaround.

- CSCub70590

  Symptom: Flapping BGP and IOSD crash occur during the LNS sessions.

  Conditions: This issue occurs during the LNS sessions.

  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.

==========tbd list by jossy==========

- CSCtz49200

  Symptom: OSPF IPv6 control packets are not encrypted or decrypted.

  Conditions: This issue occurs while configuring the IPv6 OSPF authentication.

  Workaround: There is no workaround.

- CSCtz96167

  Symptoms: QoS DSCP cases fail.

  Conditions: The symptom is observed with a QoS profile, which has DSCP as 31 configured under SBE and DSCP bit set as zero.

  Workaround: There is no workaround.

- CSCua01641

  Symptom: NAS-IP address appears as 0.0.0.0 in the RADIUS Accounting-on packet when the Cisco ASR 1002-X router is restarted:

```
*May 17 14:34:22 JST: RADIUS(0000000C): Sending a IPv4 Radius Packet
*May 17 14:34:22 JST: RADIUS(0000000C): Send Accounting-Request to 172.16.100.231:1813
id 1646/1, len 48
*May 17 14:34:22 JST: RADIUS:  authenticator F5 0C 46 BF 31 52 28 10 - 6D 9E B3 5A C8
7B 92 4D
*May 17 14:34:22 JST: RADIUS:  Acct-Session-Id     [44]  10  "00000001"
*May 17 14:34:22 JST: RADIUS:  Acct-Status-Type    [40]  6   Accounting-On
[7]
*May 17 14:34:22 JST: RADIUS:  NAS-IP-Address      [4]   6   0.0.0.0
<<=======Here!!!
*May 17 14:34:22 JST: RADIUS:  Acct-Delay-Time     [41]  6   0
*May 17 14:34:22 JST: RADIUS(0000000C): Started 3 sec timeout
*May 17 14:34:22 JST: %SYS-6-BOOTTIME: Time taken to reboot after reload =  170
seconds
*May 17 14:34:22 JST: %ASR1000_OIR-6-INSSPA: SPA inserted in subslot 0/0
*May 17 14:34:23 JST: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*May 17 14:34:23 JST: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
```

  Conditions: This issue occurs when you restart the router.

  Workaround: There is no workaround.

- CSCua20373

  Symptom: After SSO, all the GRE tunnels show that the admin is down and stay down until the SSC-600/WS-IPSEC-3 security module comes up. Complete traffic loss occurs during this time.

  Conditions: This issue occurs when vanilla GRE tunnels are configured in the system where HA and IPsec Module SSC-600/WS-IPSEC-3 card are present, and SSO is issued.

  Workaround: There is no workaround.

- CSCua21049

  Symptom: Recursive IPv6 route does not get installed in multicast RPF table.

  Conditions: There are no specific conditions for the occurrence of this symptom.

  Workaround: There is no workaround.

- CSCua21238

  Symptom: IOSD crashes are observed when **ipv6_address_set_tentative** is run.

  Conditions: This issue occurs while unconfiguring IPv6 subinterfaces.

Workaround: There is no workaround.

- CSCua29001

  Symptom: When ANCP ports are brought up to the UP,SHOWTIME state, ANCP truncation occurs only on Active RP. The downstream rate is not truncated on the standby RP, and the associated QinQ interface policy map fails to be created on the standby RP.

  Conditions: This issue occurs on the Cisco ASR1000 with "ancp truncate 32" configured.

  Workaround: There is no workaround.

- CSCua31934

  Symptoms: Crash occurs when the tunnel interface is removed from the hub and is added back again using **config replace nvram:startup-config**.

  Conditions: This symptom is observed under the following conditions:

  - It occurs one out of three times and is a timing issue.
  - DMVPN tunnel setup, where Cisco 2901 Integrated Services Router is a spoke and a Cisco ASR 1000 Series Aggregation Services Router is a hub.
  - Pass IPv4 and IPv6 traffic between the hub and the spoke for 5-10 minutes.
  - If you remove the tunnel interface on a Cisco ASR 1000 Series Aggregation Services Router and add it again using **conf replace nvram:startup-config** command, a crash will occur.

  Workaround: Use CLI to change configuration instead of the rollback feature.

- CSCua46304

  Symptom: A crash occurs at __be_nhrp_group_tunnel_qos_apply decode.

  Conditions: This issue occurs when you flap a DMVPN tunnel on the hub in a scale scenario.

  Workaround: There is no workaround.

- CSCua59573

  Symptom: A CPP crash observed in VPLS setup.

  Conditions: The issue is seen in VPLS setup.

  Workaround: There is no workaround.

- CSCua64676

  Symptom: The MVPNv4 traffic does not flow properly from the remote PE to the UUT.

  Conditions: With Agilent traffic on, the removal or addition of MDT configurations for the MVRFs configured on the UUT, MVPNv4 traffic does not flow properly from the remote PE to the UUT.

  Workaround: There is no workaround.

- CSCua85239

  Symptom: Flapping BGP sessions are seen when route-map is changed, before or after mpls-ip or mtu is configured.

  Conditions: The issue is seen between two BGP peers with matching MD5 passwords configured, and can be triggered by either of the following conditions:

  - Removing and including again route-map with mpls-ip configuration for the BGP peering on one side of the peering.
  - Removing and re-adding route-map with mtu configuration for the BGP peering on one side of the peering.

Workaround: There is no workaround.

- CSCua91473

  Symptom: A crypto_kmi_add_data_to_pyld memory leak occurs during the IPSEC key engine process.

  Conditions: This issue occurs when the IPSEC key engine's holding memory is increased.

  Workaround: There is no workaround.

- CSCub01494

  Symptom: The AD in the route installed by a client is not updated to the configured value.

  Conditions: When the **ip route 0.0.0.0 0.0.0.0 dhcp 5** command is configured, AD is not updated to 5.

  Workaround: There is no workaround.

- CSCub04112

  Symptom: The Cisco ASR 1002-X may lose OSPF routes pointing to the reconfigured OSPF interface.

  Conditions: This issue occurs during the quick removal and addition of the interface IP address.

  Workaround: Insert a short delay in between the tasks of removing or adding the IP address. The delay should be bigger than the wait interval for LSA origination, which is 500 ms by default. Refresh routing table by running the **clear ip route *** command.

- CSCub05559

  Symptom: On Cisco ASR 1001 router, after the system boots, the bootflash (eUSB) gets disconnected. As a result, the system reboots because the system cannot stay up without eUSB storage.

  Conditions: There are no specific conditions for the occurrence of this symptom.

  Workaround: There is no workaround.

- CSCub07855

  Symptom: A VRF error message occurs in the Cisco ASR 1002-X Router.

  Conditions: This issue occurs during the bootup of the router.

  Workaround: There is no workaround.

- CSCub23971

  Symptom: An access request sent by a BRAS might not contain ANCP attributes.

  Conditions: This issue is seen, if an ANCP-enabled subinterface is set up for the first time or gets removed or included again.

  Workaround: Reconfigure the ANCP neighbor name.

- CSCub31477

  Symptom: The ISG router configured for the Layer 2 connected subscriber sessions does not respond to ARP replies, after a subscriber ARP cache has expired.

  Conditions: This issue occurs when a router is configured with HSRP.

  Workaround: Clear subscriber session. After the corresponding subscriber session is reintroduced, this issue is resolved. Alternatively, configure the IP proxy ARP on the HSRP configured interface.

- CSCub69764

Symptom: After router reload, all PADIs fail on QFP and autovc stays down.

Conditions: This issue occurs intermittently, approximately once every 50 reloads, after full chassis reload.

Workaround: Reload the chassis.

- CSCub73177

  Symptom: The RP crashes.

  Conditions: This issue occurs when the Cisco 1002-X Router reloads.

  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. This issue is seen with IOS release15.2S, but not in release15.1S.

  Conditions: This issue occurs when NAT is enabled.

  Workaround: Disable NAT or downgrade to a release 15.1.

- CSCub86296

  Symptom: With OSPFv2 running between a Cisco ASR 903 router and a Cisco 7609 router, if you reset OSPF on Cisco ASR 903 router with clear ip ospf process, multiple OSPF and BFD flaps occurs, which last up to 3 minutes.

  Conditions: This issue occurs when ASR903 has BFD and static routes as BFD client.

  Workaround: Have a symmetric BFD client configuration.

- CSCub86706

  Symptom: After a multiple RP switchover, router crashes with the following message:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP HA SSO
  ```

  Conditions: This issue occurs when mVPN is with 500 VRF and multiple switchovers are performed on PE1.

  Workaround: There is no workaround.

- CSCub94825

  Symptom: After a Cisco IOS-XE bootup, there are no static reverse routes inserted as a result of applying or installing an HA crypto map. The same issue is present on the HSRP standby device, that is, the static RRI routes do not get installed when a failover occurs. The **show cry map -** command can be used to verify if RRI is enabled. The **show cry route -** command can be used to determine if RRI has occurred and if its been done correctly.

  Conditions: This issue occurs on Cisco IOS-XE 3.5 to 3.7 VRF-aware IPSec with stateless HA and static RRI IPv4.

  Workaround: Removing and re-entering the **reverse-route static** command into the configuration triggers the route insertion.

- CSCub99222

  Symptom: Standby RP reloads continuously when a RP switchover is executed on a Cisco ASR 1000 Series Aggregation Services Router as PE with about 2500 BGP sessions with IPv4 or IPv6.

  Conditions: This issue occurs on Cisco ASR 1000 Series Aggregation Services Router as PE with 2500 BGP sessions (IPv4 or IPv6).

Workaround: There is no workaround.

- CSCuc09483

  Symptoms: Under certain conditions, running a TCL script on the box, may cause software traceback and reload of the affected device.

  Conditions: This issue occurs when privilege 15 user run TCL commands that may lead to an affected device reloading.

  Workaround: There is no workaround.

- CSCuc13708

  Symptom: Cisco ASR 1000 Series Aggregation Services Router looses mapping for accounting feature on ISG users.

  Conditions: There are no specific conditions for the occurrence of this symptom.

  Workaround: The command **clear sss session all** solves the issue.

- CSCuc13992

  Symptom: The IOSD process crashes because of segmentation fault: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = PPP Events.

  Conditions: This issue occurs when BRAS functionality is configured, and the configuration includes ISG and PPPoE session termination includes ISG and PPPoE session termination.

  Workaround: There is no workaround.

- CSCuc26799

  Symptom: A Cisco ASR 1000 Series Aggregation Services Router may reload when deployed as an ISG.

  Conditions: There are no specific conditions for the occurrence of this symptom.

  Workaround: There is no workaround.

- CSCuc27343

  Symptom: The multihop L2TP tunnel fails to establish after enabling the ISG control policy under the virtual template interface for PPPoE users.

  Conditions: If the ISG control policy is not empty and the service is configured, multihop L2TP tunnel fails to establish.

  Workaround: Remove the ISG control policy.

- CSCuc33626

  Symptom: 15.2(2)S2 local policy routing issue occurs from PE to CE.

  Conditions: This issue occurs when MPLS Multi-VRF Selection with PBR is configured on PE.

  Workaround: There is no workaround.

- CSCuc40448

  Symptom: Audio fails on hair-pinned calls back from the CUBE to a SIP Provider.

  Conditions: This issue is when you upgrade to IOS release 15.2.(2)S.

  Workaround: Modify the diversion header on the transfer leg invite.

- CSCuc40585

  Symptom: Ucode crashes when GTP AIC inspects packets.

  Conditions: This issue occurs when the GTP AIC is configured.

Workaround: There is no workaround.

- CSCuc42083

  Symptom: The fman_fp Core file is displayed.

  Conditions: This issue occurs when Config GreoIPsec is configured with tunnel protection and more than 1000 route-maps are configured.

  Workaround: There is no workaround.

- CSCuc51559

  Symptom: The following message is displayed at startup:

  ```
  IOSXEBOOT-1-OOTFLASH_FAILED_MISSING
  ```

  Occasionally, upon system startup, the bootflash storage device may not be discovered by the system software. A log message to that effect is shown on the console, and after a delay, the system will reboot.

  Conditions: This occurs during normal operations of the Cisco AS 1002-X Routers.

  Workaround: No workaround is required. The system reboots itself after some delay, and the bootflash device returns to service automatically.

Note This caveat pertains to 15.2(4r)S1 ROMMON release.

- CSCub58483

  Symptom: The **radius-server attribute 6 on-for-login-auth** command is not configurable any more.

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

  Workaround: There is no workaround.

- CSCuc03831

  Symptom: The system does not save logs and the reset reason is displayed as LocalSoft.

  Conditions: This issue occurs when combined architecture platforms (ASR 1001, 2KP & Overlord, and so on) have the CC or FP sections reset the hardware.

  Workaround: There is no workaround.

- CSCub64168

  Symptom: On the Cisco ASR 1001 router, bootflash disconnects and reconnects. As a result, there is loss of bootflash contents.

  Conditions: This issue occurs after approximately 64 reloads of the Cisco ASR 1001 router.

  Workaround: There is no workaround.

- CSCub01494

  Symptom: The AD in the route installed by a client is not updated to the configured value.

  Conditions: When the **ip route 0.0.0.0 0.0.0.0 dhcp 5** command is configured, AD is not updated to 5.

  Workaround: There is no workaround.

- CSCuc40682

  Symptom: The active RP crashes on the LNS with the Process SSS Mgr when the LAC is reloaded.

Conditions: This issue occurs when the LAC is reloaded.

Workaround: There is no workaround.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.1S

This section documents resolved issues on Cisco ASR 1000 Series Aggregation Services Routers Release 3.7.1S.

- CSCua27722

  Symptom: The Netflow TimeStamp may show time drift compared to NTP time. This effect is equal to approximately 50 seconds of lost time per day.

  Conditions: This issue occurs when the flexible Netflow runs on either an ESP40-based Forwarding Processor or on a Cisco ASR 1001 router.

  Workaround: There is no workaround, but when the time skew exceeds 10 minutes, Netflow TimeStamp self-corrects.

Note This caveat pertains to 15.2(4r)S1 ROMMON release.

- CSCsz65576

  Symptom: One or more linecards may fail to boot in a Cisco ASR 1000 router with an RP2 or there may be an error with the EOBC. %CMFP-3-STANDBY_EOBC_LINK_ERROR: F0: cman_fp: Standby EOBC link error detected.

  Conditions: This issue is observed with certain combinations of RP2 and ESP10.

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

- CSCti62247

  Symptom: If a packet is sent to a null interface, an Cisco ASR 1000 router does not respond with an ICMP packet.

  Conditions: This issue occurs when a prefix is routed to the null interface.

  Workaround: There is no workaround.

- CSCtt19856

  Symptom: On the ASR1000, while making changes to the *ppp multilink fragmentation <size>* parameter on the Virtual-Template, the resulting change is reflected in IOS on the active bundles (**show ppp multilink <interface>**). However, the QFP does not reflect this change (**show platform hardware qfp active feature mlppp datapath bundle <int> detail**) at the time of the command's issuance. MLPPP fragment size remains at the previous setting, potentially impacting performance and operation in the network.

  Conditions: This issue occurs when the MLPPPoBB subscribers change the value of the **ppp multilink fragmentation <size>** parameter set on the Virtual-Template.

  Workaround: Any MLPPPoBB subscribers using the Virtual-Template that was changed should be flapped to pick up the new value.

- CSCtt95532

  Symptom: POS Netsync, QL status goes to QL-INV0 after reconfiguring the network-clock input.

Conditions: QL-Value goes to QL-INV0 after reconfiguring the POS interface for network-clock input.

Workaround: There is no workaround.

- CSCtw53516

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

  Conditions: This issue occurs when **shut** is run on the interface on CE1.

  Workaround: There is no workaround.

- CSCty05282

  Symptom: After some reloads, the last reload reason in **show version** output is seen as LocalSoft.

  Conditions: The conditions under which these symptom is observed is unknown.

  Workaround: There is no workaround.

- CSCty37836

  Symptom: ceqfpMemoryResourceTable does not include DRAM values.

  Conditions: This issue occurs when ceqfpMemoryResourceTable is queried.

  Workaround: There is no workaround.

- CSCty41336

  Symptoms: Forward-alarm ais does not work on CESoPSN circuits.

  Conditions: This symptom occurs when you create SAToP and CESoPSN circuits and configure forward-alarm ais.

  Workaround: There is no workaround.

- CSCty42453

  Symptom: Pending acknowledgment is seen in int ATM.

  Conditions: This issue is observed while oir reloads.

  Workaround: There is no workaround.

- CSCty55408

  Symptom: Pending issues and acknowledgments are observed after unconfiguring and then reconfiguring the same scale configuration while traffic is running.

  Conditions: This issue occurs after configuring four overlays with 500 EFPs per overlay, setting up the traffic as described in the DDTS start traffic, removing the overlay and EFP config, and copying the same config back on one of the otv routers.

  Workaround: There is no workaround.

- CSCty84235

  Symptom: Traceback IOSXE_FMANRP-4-MSGDISPATCH: Unable to dispatch received TDL messages from Forwarding Manager.

  Conditions: This issue occurs while disconnecting ISG sessions and removing configuration.

  Workaround: There is no workaround.

- CSCtz32360

Symptom: After bootup or initial interface configuration, an ASR1002 router with Sync-E SPA may indicate an interface an "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 show amber.

Conditions: This issue is observed primarily after booting the device, 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> 2048kCLI when the clock is not fed to the port. Once the clock is fed, then the lockout can be cleared using the network-clock clear lockout port 2048k CLI.

- CSCtz40431

  Symptom: Bandwidth reamining percent command does work unless the session is broken and reestablished.

  Conditions: This issue occurs when the bandwidth reamaining ratio of one session is more than one.

  Workaround: There is no workaround.

- CSCtz70973

  Symptom: Unexpected reload of Cisco ASR1002-X router or ESP100 occurs.

  Conditions: This issue is typically observed when large numbers of interfaces are present.

  Workaround: There is no workaround.

- CSCtz74060

  Symptom: The output of the **show platform hardware qfp active feature ess state** command is showed in XML format during ISSU subpackage downgrade from XE3.7.0 to earlier releases on Cisco ASR 1004 router. This issue does not impact functionality.

  Conditions: This issue occurs during an ISSU subpackage downgrade.

  Workaround: There is no workaround.

- CSCtz74310

  Symptom: Netsync fails on a Maverick or CEOP_24xT1E1.

  Conditions: There are no specific conditions for the occurrence of this symptom.

  Workaround: There is no workaround.

- CSCtz74315

  Symptom: Metronome SPA is not supported on ASR1002-X. Netsync feature is supported on Hybrid SPA.

  Conditions: There are no specific conditions for the occurrence of this symptom.

  Workaround: There is no workaround.

- CSCtz91271

  Symptom: QFP BQS schedule move to new output interface on different subdevice is unsupported. QoS for this schedule is disabled.

  Conditions: This issue occurs when tunnel target output interface changes from a target associated with one QFP subdevice on ESP100 to a target associated with another QFP subdevice.

  Workaround: Restore failed link or route so that schedule is moved back and QoS is restored. Alternatively, force the schedule to fail back to a link that is on the same subdevice the schedule was originally on.

- CSCtz99914

  Symptom: Traffic drops occur on MLP interfaces with QoS after system reload.

  Conditions: This issue occurs after reload.

  Workaround: Shut/no shut the multilink bundle after reload if seeing tail drops on the interface.

- CSCua08206

  Symptom: VCs that are configured with VPLS on the standby RP appear in down state.

  Conditions: This issue occurs during core link flap.

  Workaround: Run the **clear xcon all** command.

- CSCua13418

  Symptoms: RP-Announce packets are replicated across all the tunnel interfaces and the count of replication is equal to the number of tunnel interfaces. For example, if there are 3 tunnel interfaces, then each tunnel should forward 1 RP-Announce packet each minute (with the default timer configured). However, in this case, each tunnel is forwarding 3 RP-Announce packets across each tunnel interface. This issue is not specific to the number of interfaces. It can happen with any number of tunnel interfaces.

  Conditions: This symptom is observed when filter-autorp is configured with the **ip multicast boundary** command. This issue is seen on the Cisco 3725 router too, where the incoming packets are being replicated because of the **filter-autorp** command.

  Workaround: Removing filter-autorp resolves the issue. However, you need to remove the **pim** and **boundary** commands first and then reapply the pim and boundary list without the **filter-autorp** keyword. Also, doing this might lead to redesigning of the topology to meet specific requirements. int Tun X no ip pim sparse-dense mode no ip multicast boundary XXXXXX filter-autorp int TuX ip pim sparse-dense mode ip multicast boundary XXXXXX.

- CSCua16899

  Symptom: SFP and SPA modules may appear to be missing from "show inventory"

  Conditions: This has been observed after system boot up

  Workaround: Reload of SIP should reinitialize SPA and SFP modules.

- CSCua24227

  Symptom: cpp_cp_svr crashes when issuing **sh plat hard qfp act infra bqs stat** CLI.

  Conditions: No QoS service-policy configuration causes this crash. Running the CLI show command also causes the crash.

  Workaround: Do not use the **sh plat hard qfp act infra bqs stat** command.

- CSCua25041

  Symptom: entPhysicalIsFRU of 6-port Built-in GE SPA in ASR1002-X is false.As a result built-in spa is shown in cefcModuleTable.

  Conditions: When snmp query is done on entPhysicalIsFRU/cefcModuleTable on ASR1002-X Chassis.

  Workaround: None

- CSCua26487

  Symptoms: SNMP loops at OID 1.3.6.1.4.1.9.9.645.1.2.1.1.1, and as a result, SNMP walk fails.

  Conditions: This symptom is observed only on the SNMP getbulk request on 1.3.6.1.4.1.9.9.645.1.2.1.1.1.

Workaround: Exclude the MIB table from SNMP walk using SNMP view. See the below configurations. snmp-server view <view name> iso included snmp-server view <view name> ceeSubInterfaceTable excluded snmp-server community <community> view <view name>nterfaceTable excluded snmp-server community <community> view <view name>

- CSCua27537

  Symptom: ISSU one shot does not work on older 2RU chassis.

  Conditions: This only happens on older 2RU chassis, not on our latest 2RU Fixed chassis.

  Workaround: Run standard ISSU procedure on these 2RU chassis.

- CSCua27842

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

  Conditions: This symptom occurs when the Cisco ASR 1000 router acts as the MPLS L3VPN UHP. It crashes because FW/NAT requires the l4_info to be set.

  Workaround: There is no workaround.

- CSCua28910

  Symptom: vrf flap with ipv6 mtu configuration causes ipv6 table id disabled and packets dropped

  Conditions: config ipv6 mtu 1280 under interface change interface vrf

  Workaround: Remove ipv6 mtu 1280 or change mtu to any other value

- CSCua32893

  Symptom: Ucode and cpp_cp_svr crash seen on ASR 1002 (standby) while scaling to 0.5 million NAT64 translation.

  Conditions: This issue is seen with high scaling.

  Workaround: There is no workaround.

- CSCua34428

  Symptom: When routed port is configured, the cc messages are not generated as the local mep is in I state instead of Y state for cc messages. Hence rmep was not learnt.

  Conditions: This issue occurs while applying router port.

  Workaround: Perform shut/no shut opearation.

- CSCua41828

  Symptom: sh ipv6 traffic counter shows a larger number of sent neighbor unreachables than were actually sent.

  Conditions: This occurs when a packet with a link-local source address and whose destination address is in a remote network is received by a Cisco ASR router.

  Workaround: There is no workaround.

- CSCua45303

  Symptom: Bogus cloned sessions in PD after hitting QFP memory exhaustion.

  Conditions: With 128K lite-sessions churning under load, clearing the default session can lead to QFP memory exhaustion. When this happens, bogus cloned sessions are seen in PD.

  Workaround: There is no workaround.

- CSCua48243

  Symptom: ASR1K logs truncated IPv6 addresses if "log" keyword is used in a security ACL.

Conditions: Security ACL with "log" keyword applied on an interface

Workaround: There is no workaround. ACL's functionality is not affected.

- CSCua49474

  Symptom: Some TCP segments of particular length may be forwarded with wrong packet payload if NAT is configured.

  Conditions: This issue is caused by NAT-configured packets are TCP segments of particular length.

  Workaround: configure *ip tcp adjust-mss* to a smaller value than the current tcp flow.

- CSCua49782

  Symptom: Tracebacks are observed.

  Conditions: configure/unconfigure overload match-in vrf in quick succession

  Workaround: Do not config/unconfig in quick succession.

- CSCua51775

  Symptom: Adding flow-based fair-queue command to QoS policy-map might cauase conditional priority fail to police the traffic when congestion condition happens.

  Conditions: If the service-policy has already been attached to interface, then adding the "fair-queue" command to policy-map might lost the congestion detection flag setting which is used by conditional priorirty traffic class. And this traffic class would behave like strct priority traffic class.

  Workaround: Detach then re-attached the same service-policy to interface when need to add "fair-queue" command to the policy-map already attaching interface.

- CSCua52064

  Symptom: LSMPI-4-INJECT_FEATURE_ESCAPE: Egress IPV6 packet delivered inject path

  Conditions: Traceback seen when we disable "ipv6 unicast-routing" from the device which 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 "clear subscriber session all" is issued while EAPSIM, L3 Web Authen, and Walkby sessions are establishing concurrently.

  Conditions: EAPSIM, L3 Web Authen, and Walkby sessions are establishing concurrently. Issue is reproducible with only a couple thousand sessions up.

  Workaround: None.

- CSCua53659

  Symptom: Performance drop in ESP100

  Conditions: More then 20% Performance degradation seen with large packet size.

  Workaround: None

- CSCua58072

  Symptom: IPv6 BGP next hop gest collected with mis-oderered bytes (for example, non-existing IPv6 address is displayed for it)

  Conditions: This issue occurs on some ESP40 devices.

  Workaround: There is no workaround

- CSCua58324

  Symptom: Pending objects are generated after copying a pwlan config with default sessions to running-config.

  Conditions: Boot ASR1K wit basic startup-config. Copy the pwlan config to running-config. Note the pending objects afterwards.

  Workaround: There is no workaround.

- CSCua58324

  Symptom: Pending objects are generated after copying a pwlan config with default sessions to running-config.

  Conditions: Boot ASR1K wit basic startup-config. Copy the pwlan config to running-config. Note the pending objects afterwards.

  Workaround: None

- CSCua59268

  Symptom: When an ESP switchover happens in an intra or inter box setup, sometimes the standby ESP gets stuck and does not come up properly.

  Conditions: The **show redundancy application group** <*grp-number*> command shows the RF state as STANDBY COLD-BULK.

  Workaround: This issue can be solved by reloading the standby.

- CSCua66386

  Symptom: ASR1000 does not send ICMPv6 unrechable code 1 message to sender when packets are discarded by ACL.

  Condition: -use ASR1000 as LNS -deny the packets by ACL in the virtual-template

  Workaround: There is no workaround.

- CSCua68211

  Symptom: Sub-classification of HTTP traffic (for example, by host or url) does not work on the first transaction of the HTTP flow and matches on the second request.

  Conditions: Only happens when all protocols or specific protocols on top of HTTP are enabled - sharepoint, audio-over-http, video-over-http, windows-azure, oracle-ebsuite-unsecured, bittorrent

  Workaround: If you are using subclassification on HTTP, avoid using protocol discovery, FNF or specifically enabling other protocols which run over HTTP.

- CSCua68825

  Symptom: ASR configured as LISP xTR might generate ICMP too big messages with wrong source address.

  Conditions: When data packets are encapsulated by LISP xTR and the encapsulated packet is greater than the egress MTU, then the ASR generates the ICMP reply with wrong source address.

  Workaround: None.

- CSCua69725

  Symptom: Pending objects and traffic loss occur on cell packed interfaces.

  Conditions: This issue occurs during router reload.

  Workaround: Reload the router.

- CSCua70307

Symptom:When volume based lifetime expires, IPsec session goes down for a few seconds during rekey.

Conditions: User config volume based ipsec lifetime bigger than 100GB

Workaround: Use default lifetime (4GB), or any value < 100GB, or disable volume based lifetime.

- CSCua70906

  Symptom: Performance for NAT is suboptimal when run on ESP100

  Conditions: When on Run on ESP100 on release XE3.7.0. Note NAT is not officially supported on XE3.7.0 on ESP100. NAT support on ESP100 starts with XE3.7.1.

  Workaround: Upgrade to XE3.7.1 or later (i.e. to a supported release).

- CSCua71239

  Symptom: RP may crash when executing the CLI command: <CmdBold>show platform software ess rp active data-base lite_session record

  Conditions: The crash is seen if no IP lite sessions exist in the system.

  Workaround: There is no known workaround besides avoiding this particular CLI command.

- CSCua72048

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

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

  Workaround: There is no workaround.

- 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: none

- CSCua79516

  Symptoms: SYN packets to establish ftp-data connections are sporadically dropped at the Cisco ASR router.

  Conditions: This symptom is observed under the following conditions:

  - Using the active mode FTP.
  - Using PAT.

  The symptom is observed on Cisco ASR 1000 Series Aggregation Services Routers.

  Workaround 1: Use the passive mode FTP. Workaround 2: Use the static NAT/dynamic NAT configuration.

- CSCua84263

  Symptom: profile is called instead of editor

  Conditions: no cli is run at adj mode

  Workaround: set the correct value at adj mode instead of no cli.

- CSCua85116

  Symptom: Under certain conditions, ESP may reload and ESP forced switchover may happen.

Conditions: This issue 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.

- CSCua88412

  Symptom: DNS queries through ASR1K NAT sessions are not being resolved even though 'no ip nat service dns-reset-ttl' has been configured.

  Conditions: ASR1K Configuration includes 'no ip nat service dns-reset-ttl'.

  Workaround: Remove and re-add the 'no ip nat service dns-reset-ttl' configuration or if the target platform supports it reload the ESP(s).

- CSCua90577

  Symptom: VRF-aware IP SLA with ICMP probes fail.

  Conditions: The Cisco ASR 1000 Series Aggregation Services Router, which is PE, 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 continues failures. Manual Ping via CLI fails as well.

  Workaround: The workaround is to shut/unshut the ICMP source interface (Loopback) or deconfigure and reconfigure the VRF on the loopback interface. If the router is being reloaded, the same problem is seen again.

- CSCua91995

  Symptom: IPv6 IPsec sessions may come up slow (1 TP per 10 seconds)

  Conditions: When IPv6 address are identical in first few bytes.

  Workaround: There is no workaround.

- CSCua92557

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

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

  Workaround: To resolve this issue, use static NAT.

- CSCua93149

  Symptom: Platform Kernel message when we enable network-clock synchronization on ASR1002-X.

  Conditions: After configuring 'network-clock synchronization' on ASR1002-X platform level kernel messages are seen on the console.

  Workaround: There is no workaround.

- CSCua96209

  Symptom: Dropped fragments are observed.

  Conditions: This issue occurs with fragmented traffic in CGN mode.

  Workaround: There is no workaround

- CSCua97509

  Symptom: ESP80 Crash observed

Conditions: High scale configs of VPLS and L2VPN with traffic. When we ESP switchover followed by RP SSO , ESP crash is observed

Workaround: None

- CSCua99060

  Symptom: Back to back FR is observed.

  Conditions: This issue occurs when the router is reloaded.

  Workaround: Perform shut/no shut the FR interface.

- CSCua99409

  Symptom: ESP reload with fman-fp error occurs.

  Conditions: This issue occurs when crypto map from interface is unconfigured and there is double ACL in the crypto map

  Workaround: There is no workaround.

- CSCub00134

  Symptom: CPP CP svr messages seen on the CP server logs

  Conditions: on checking the cp server logs on normal conditions

  Workaround: none

- CSCub00822

  Symptom: Output of **show sbc call-stats all current** always shows as 15 minutes.

  Conditions: This issue occurs when adjacencies are more in numbers with running calls.

  Workaround: There is no workaround.

- CSCub01576

  Symptoms: ESP reloads on the Cisco ASR 1000 Series Aggregation Services Routers due to ucode crash.

  Conditions: This symptom is observed on the Cisco ASR 1000 router where the Layer 4 Redirect feature is configured. This problem was first introduced in Cisco Release 15.2(01)S. This issue may be not seen at all in some customer environments to about once a week in medium-sized high CPS ISG production networks.

  Workaround: There is no workaround.

- CSCub01816

  Symptom: ESP CPP crash with the Pfr

  Conditions: This problem will occur when there are a lot of learn lists

  Workaround: No known Workaround

- CSCub03744

  Symptom: ESP100 crashes.

  Conditions: Removing a hierarchical QoS policy-map from a port-channel member link.

  Workaround: None.

- CSCub07430

  Symptom: icmp echo-reply with the wrong src ip address from the asr1k

  Conditions: MPLS Multy-VRF Selection with PBR is configured

Workaround: There is no workaround.

- CSCub07679

  Symptom: The router may crash or generate datapath trace-back.

  Conditions: This issue occurs when one of the following conditions is met: 1. MMON (Media Monitoring) is enabled. 3. NBAR is enabled and NBAR is configured to look into IPv6 tunnels, using the one or both of the following CLI commands: a. ip nbar classification tunneled-traffic ipv6inip b. ip nbar classification tunneled-traffic teredo

  Workaround: 1. Disable MMON. 2. Disable NBAR classification of tunneled traffic: # no ip nbar classification tunneled-traffic ipv6inip # no ip nbar classification tunneled-traffic teredo

- CSCub08714

  Symptom: Poor performance for multicast on asr1k over dmvpn

  Conditions: 1) Multicast packet has to be coming in on a Tunnel interface (not a physical interface). 2) NS (negate signaling) flag has to be set on one of the interfaces in the MFIB (S,G) entry. If both these conditions are met, then the packet is punted to control plane & 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: None

- CSCub13697

  Symptom: In very rare scenarios, embedded IP addresses in SIP packets may not get fixed up as expected.

  Conditions: This was first identified on an ASR1K running 15.1(3)S3. The soft switch inside had static PAT configured for tcp and udp port 5060 to a mapped IP address A. The same soft switch on the inside also bridged media and ASR was configured with dynamic PAT overload to a mapped address B. Inbound and Outbound connection must be configured to use different mapped IP address.

  Workaround: Use static 1-1 NAT for the soft switch on the inside.

- CSCub16403

  Symptom: On the ASR1K series of routers running the Flexible Netflow feature, when the command "show flow monitor MON cache" is issued timestamps are displayed as local wallclock time. These timestamps may be skewed by the time delta between how long the Route Processor (RP) has been up and how long the Forwarding Processor (FP or ESPXX) has been up. This delta is typically in the range of several minutes but it may be even longer than that.

  Conditions: ASR1K router running Flexible Netflow when show flow monitor MON cache command is issued.

  Workaround: None.

- CSCub17585

  Symptom: System crash and reboot occur with AVC1.0.

  Conditions: This issue occurs when FNF collects HTTP fields such as host, for example, with AVC1.0. The crash occurs infrequently in context of MSN traffic.

  Workaround: Remove the HTTP fields from the FNF records.

- CSCub18741

  Symptom: Fragmented SIP packets may be dropped due to FirewallInvalidZone.

Conditions: This issue occurs when NAT and Firewall is configured in VASI interface. In such a case 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.

- CSCub19254

  Symptom: The statistics on Kingpin Hybrid SPA shows 4 bytes extra in each egress packet

  Conditions: Send traffic to hybrid spa that needs to be switched. The ingress has n octets and egress has n 4 octects shown in statistics.

  Workaround: There is no workaround.

- CSCub19477

  Symptom: Default sessions do not establish when you apply VRF as a service to the default policy. VRF can only be applied to a default session by assigning a VRF on the access-interface. However with dedicated sessions, one cannot apply a VRF on the access-interface and VRF transfer at the same time. Thus if we require VRF transfer on dedicated sessions, we need VRF transfer on lite sessions as well.

  Conditions: This issue occurs when access-side interface is in the default VRF, VRF is applied as a service to the default policy.

  Workaround: There is no workaround.

- CSCub23298

  Symptom: Multicast traffic over PVC Bundle always goes to prec 0 pvc.

  Conditions: This issue occurs when multicast over PVC bundle is configured.

  Workaround: There is no workaround.

- CSCub25280

  Symptom: Same inside global addresses could be assigned to multiple inside local addresses with dynamic route-map configuration and ALG traffic.

  Conditions: ALG traffic dynamic route-map configuration

  Workaround: Use static/dynamic NAT configuration w/o route-maps

- CSCub25362

  Symptom: FP crashes with certain mulitcast config, on reloading the Cisco ASR 1000 router with RP2.

  Conditions: This issue occurs when the router is reloaded.

  Workaround: There is no workaround.

- CSCub25419

  Symptom: The Cisco ASR 1000 router ESP may crash at pfr_tt_ll_resp_cb when 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 solves this issue.

- CSCub25542

  Symptom: Blacklist could not be deleted or expired.

  Conditions: All

Workaround: Reboot the box

- CSCub27029

  Symptom: The command **sh ip nat trans** causes error message or crash.

  Conditions: There are no specific conditions for the occurrence of this symptom.

  Workaround: Downgrading to any version earlier than XE3.6.0 release solves the issue.

- CSCub27590

  Symptom: RP crash on EXEC process

  Conditions: Removing/re-adding BGP AD l2 vfi with debug enabled

  Workaround: None

- CSCub32890

  Symptom: Request to include the max support user-queue info for the following comamnd output: 'sh platform hardware qfp active infrastructure bqs capabilities'

  Conditions: Current show bqs capability command output doesn't include this info.

  Workaround: None.

- CSCub33850 tbd

  Symptom:

  Conditions:

  Workaround:

- CSCub34128

  Symptom: Ucode crash occurs followed by FP crash seen on sending GTP traffic.

  Conditions: This issue occurs while sending traffic from SGPRS simulator.

  Workaround: There is no workaround.

- CSCub35526

  Symptom: The **plim qos input queue** command reflects on all int of the same spa.

  Conditions: The configuration reflects for all the interfaces on the spa.

  Workaround: There is no workaround.

- CSCub36301

  Symptom: BFD sessions go down during FP switchover.

  Conditions: This issue occurs when the peer is a Cisco ASR 1000 router with large BFD sessions.

  Workaround: There is no workaround.

- CSCub39131

  Symptom: Packets are dropped.

  Conditions: This issue occurs with 5 cps basic sip call.

  Workaround: Reduce the traffic load from 5 cps to 2 cps.

- CSCub44215

  Symptom: In routed vpls scenario, when BDI interface on an ASR1002 is configured in vrf and receive packets on vpls VFI (from a PE router with xconnect) destined to vpn prefixes imported via route-target import from it's l3vpn mpbgp peer(another PE), it corrupts the packets. The destination device drop all the packets as it contains ip option.

Conditions: The issue only happens for destination learned via route-target import policy. The devices behind the PE(having xconnect) can ping he BDI interface fine and the routes directly connected on ASR or learned via another device in the same vrf. The issue is seen in 15.2(2)S1 and 152-4.S.bin.

Workaround: There is no workaround.

- CSCub46238

  Symptom: FP crash

  Conditions: Booting the router

  Workaround: None

- CSCub51279

  Symptom: The Cisco ASR 1000 router resets its FP with FW NAT feature combination.

  Conditions: There are no specific conditions for the occurrence of this symptom.

  Workaround: There is no workaround.

- CSCub52639

  Symptom: Embedded IP addresses in SIP packets may not get translated

  Conditions: Different NAT mappings to translate the same ip address in the header and payload

  Workaround: Use same configuration for both header and embedded translation for the same ip address.

- CSCub53087

  Symptom: High number of GTPv0 and GTPv1 packet drops occur with "GTP permit-error" OFF. On ASA, this feature can be turned ON.

  Conditions: This issue occurs with zone-based firewall for GTP traffic configured and GTP permit-error OFF.

  Workaround: There is no workaround.

- CSCub53699

  Symptom: ESP crashes with FNF monitor contains Extracted fiels like HTTP URL.

  Conditions: FNF monitor with Extracted fiels.

  Workaround: None

- CSCub54686

  Symptom: HS_logger crashes with IPFIX export of long URL

  Conditions: This issues occurs when long URLs are present.

  Workaround: There is no workaround.

- CSCub55036

  Symptom: Combination of static NAT and Firewall allows flow of ICMP timestamp even though user defined in ACL to drop.

  Conditions: NAT with Firewall for ICMP timestamp flow

  Workaround: Apply ACL on interface deny ICMP time-stamp request.

- CSCub55948

  Symptom: The Cisco ASR 1000 router crashes due to fragmented ICMP packets on BDI5.

  Conditions: There are no specific conditions for the occurrence of this symptom.

Workaround: 1. Increase the MTU size at adjacent router which is connected with this ASR. 2. Under the interface BDI, use access-list to deny those icmp packets destined to subnet broadcast address.

- CSCub57735

  Symptom: "ip nat inside source route-map NAT-MAP pool xyz force" could not be removed it is said Dynamic nat in use even when there's no nat entries at all

  Conditions: 1) Configure dynamic NAT 2) make SIP traffic, which hits NAT entries 3) stop test, clear nat entries, and remove cli

  Workaround: use "no ip nat inside source route-map NAT-MAP pool xyz force" instead

- CSCub58238

  Symptom: FP crashes on loading ATM VC bundle configuration

  Conditions: The issue is seen on configuration around 200 ATM VC bundles.

  Workaround: There is no workaround. FP stabilizes after the initial crash.

- CSCub58991

  Symptom: ASR1000 "show ppp multilink" command did not display the correct configuration status for MLPPP Fragmentation, Interleaving, and Distributed MLPPP platform status. ASR1000 was also enabling Multilink PPP fragmentation (legacy mode) enabled by default. Should only be enabling fragmentation if explicitly configured on the Multilink bundle interface or Virtual-Template (Broadband MLPPP).

  Conditions: All Multilink PPP configurations.

  Workaround: None

- CSCub59275

  Symptom: Config of CT3 controller Serial intfs doesn't match between and standby RPs. Many error messages like - : %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 standby RP during controller configuration. IP addresses are assigned to wrong Serial interfaces. On RP switchover, because of the mismatch, traffic doesnt pass

  Conditions: Configuring CT3 SPA in a dual RP router

  Workaround: none

- CSCub62988

  Symptom: Consecutive crashes occur.

  Conditions: This issue occurs on a Cisco ASR 1000 router with ESP10 with IOS 15.2(2)S release.

  Workaround: There is no workaround

- CSCub64068

  Symptom: "CPPOSLIB-3-ERROR_NOTIFY F0: cpp_cp: cpp_cp encountered an error" log message with tracebacks. This can result in a ESP crash or control plane/configuration events not getting processed on the ESP.

  Conditions: Combination of ESP20 or ESP40 and CC40 installed in an ASR1006 or ASR1013 platform and the CC40 does not have SPAs in stalled in bay 0 or 2 and bay 1 or 3.

  Workaround: If you have two or more SPAs installed in the CC40, ensure there is a SPA in bay 0 or 2 and bay 1 or3. If you only have 1 SPA installed in the CC40, there is no workaround.

- CSCub64398 tbd

Symptom:

Conditions:

Workaround:

Workaround: There is no workaround.

- CSCub66569

  Symptom: ASR1000 may generate IGMP packets which have all zero source MAC address.

  Conditions: Configured OTV ED/Bridge-domain.

  Workaround: None.

- CSCub66957

  Symptom: ESP40 crashes when traffic hits the router.

  Conditions: This issue occurs on basic LSM setup of PE-P-PE.

  Workaround: Disabling LRE fixes the issue.

```
set plat hard qfp active feature multicast v4 lre off
set plat hard qfp active feature multicast v6 lre off
```

- CSCub68200

  Symptom: FP may crash while flapping sessions with ISG services, or flapping the ISG services themselves.

  Conditions: This behavior might be seen on a Cisco ASR 1000 router running 15.1(2)S images or later. The ISG services involved must be Traffic Class services, and they may have any of L4R, DRL/Policing, or accounting-based features applied. The behavior may be seen when such services are quickly added and removed from a subscriber.

  Workaround: There is no workaround.

- CSCub70706

  Symptom: Router crashes when binding a monitor to an interface after binding more than 3 exporters to the monitor.

  Conditions: The crash occurs when the router runs out of memory during the bind process and the binding is being reverted.

  Workaround: Do not exceed the recommended limit of DRAM for FNF config.

- CSCub70819

  Symptom: There is no way for customers to upgrade existing throughput licenses. (ex. from throughput_10g to throughput_20g)

  Conditions: None

  Workaround: Customers can only get the throughput value by installing the corresponding exact throughput license.

- CSCub72677

  Symptom: FP crash seen

  Conditions: when flapping single link PPP sessions with QOS

  Workaround: None

- CSCub73403

  Symptom: Bad voice quality is observed.

Conditions: This issue is observed on RP1, ESP10, or SIP10 when there are multiple spas present and transcoding is active.

Workaround: There is no workaround.

- CSCub75461

  Symptom: The following traceback is observed after RP2 switch-over event.

  %CPPTCAMRM-6-TCAM_RSRC_ERR: F1: cpp_sp: Allocation failed because of insufficient TCAM resources in the system.

  Conditions: ASR1000 series router with redundant RP2's and ESP forwarding processor. The ESP's TCAM resources must be nearly exhausted and a RP2 switch-over is executed.

  Workaround: There is no workaround.

- CSCub83960

  Symptom: After the second RP switchover, mcast traffic stops forwarding by PE.

  Conditions: This issue occurs in mVPN topology, during mcast traffic sending, while performing RP switchover on PE1.

  Workaround: Use **clear ip mroute *** command to make the global MDT mroute re-built can restore mcast traffic before/after the second switch-over.

- CSCub84204

  Symptom:GTPv0 request dropped and failed to create session

  Conditions: All

  Workaround: None

- CSCub85159

  Symptom: GTPv0 request drops and fails to create session.

  Conditions: There are no specific conditions for the occurrence of this symptom.

  Workaround: There is no workaround.

- CSCub91150

  Symptom: Ping to SBC interface from a Cisco ASR 1000 router fails.

  Conditions: This issue may occur in any of the following conditions:

  - SBC interface is created with netmask /32
  - SBC is activated

  Workaround: Deactivate sbc, delete sbc interface, and re-create it again.

- CSCub93228

  Symptom: Traffic not passing even it matches the filter condition

  Conditions: IPv4 and IPv6 co-exist in the interface configuration and with FW NAT configured.

  Workaround: Not real workaround but could the following. Instead of using pre-natted source address in ACL, use post-nat source address. E.g. If the following static nat is used, ip nat inside source static 36.1.1.2 37.1.1.83 In order to allow traffic from host 36.1.1.2 to pass thru fireall, the ACL should be like:

  ```
  ip access-list extended foo-list                    permit ip host 36.1.1.2 any    Due
  to this list, the acl can be configured as follows to workaround the issue:
  ip access-list extended foo-list                     permit ip host 37.1.1.83
  ```

- CSCub94985

Symptom: CHSTM (prowler) spas serial interface shows down due to C2 byte mismatch.

Conditions: This issue is seen in releases 15.2(01)S, 15.2(02)S and 15.2(04)S.

Workaround: There is no workaround.

- CSCub95951 tbd

- CSCub96509

  Symptom: Priority traffics are dropped

  Conditions: With model3/model4 configs on GEC links.

  Workaround: N/A

- CSCub96576

  Symptom: Reload may occur on a Cisco ASR 1000 router NAT.

  Conditions: This issue may occur while removing static rmap mapping.

  Workaround: There is no workaround.

- CSCub97070

  Symptom: Standby RP took 19 minutes to STANDBY HOT state after super package downgrade from XE3.7.1 throttle to XE3.7.0 / XE3.6.2 / XE3.5.2 CCO. Standby RP took 19 minutes to STANDBY HOT state after super package upgrade from XE3.7.1 throttle to XE3.8.0 throttle / mcp_dev.

  Conditions: On dual-RP platform super package ISSU test only.

  Workaround: None

- CSCub99205

  Symptom: Mod F: Shaper becomes inactive when policy-map is removed and added back on a subinterface.

  Conditions: This issue occurs when policy-map is removed and added back on a subinterface.

  Workaround: Changing shaper value reactivates shaper.

- CSCuc02921

  Symptom: ESP crash.

  Conditions: When SYN cookie protection is being triggered, and the packet TCP data offset is wrong.

  Workaround: Do not configure SYN cookie protection.

- CSCuc05660

  Symptom: Any DNS queries being NAT'd that have cname entries in the payload get the DNS TTL set to zero.

  Condition: This issue occurs during DNS querying.

  Workaround: There is no workaround.

- CSCuc06286

  Symptom: Fman-fp crashes Stateful Swichover

  Conditions: Router has scaled vpls configuration and the issue happens on SSO switchover.

  Workaround: None

- CSCuc10081

  Symptom: Upgrade or downgrade ISSU fails.

  Conditions: This issue is seen on devices with versions 3.7.x or later.

  Workaround: There is no workaround.

- CSCuc13500

  Symptom: CPP Crashes seen on Active and Standby FP following RP switchover.

  Conditions: This issue occurs after RP switchover.

  Workaround: There is no workaround.

- CSCuc16623

  Symptom: After changing the grandparent shape rate through ANCP, traffic is not shaped to the new rate.

  Conditions: This issue occurs on PPPoE model F Qos.

  Workaround: There is no workaround.

- CSCuc26434

  Symptom: RP information is not learned when Auto-RP is configured and the MA and RP candidate are on different PE.

  Conditions: This issue occurs when MA and RP candidate are on different PE.

  Workaround: There is no workaround.

- CSCsq83006

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

  Conditions: The symptom occurs with full mesh four routers which are connected via port-channels. Additionally, it occurs with over five routers which 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>
  ```

- CSCtg47129

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

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

  Workaround: There is no workaround.

- CSCto87436

  Symptom: A Cisco device running IOS may crash due to a watchdog timeout with the following error messages:

  ```
  %SYS-3-CPUHOG: Task is running for (126004)msecs, more than (2000)msecs (30/1),process
  = SSH Process. -Traceback= 0x63D827CCz 0x6496A670z 0x649774CCz 0x649776A0z 0x6497777Cz
  0x6496BCFCz 0x6496BEA4z 0x6496BFF8z 0x61E122A0z 0x61DFC6CCz 0x61DFCF94z  0x61DFF270z
  0x61DFC5F8z 0x61E980E0z 0x61E984ACz 0x61E3DF6Cz  %SYS-3-CPUHOG: Task is running for
  (128004)msecs, more than (2000)msecs  (31/1),process = SSH Process. -Traceback=
  0x63D7AA5Cz 0x62A47F68z 0x62A48500z 0x62A45F9Cz 0x649774E8z  0x649776A0z 0x6497777Cz
  0x6496BCFCz 0x6496BEA4z 0x6496BFF8z 0x61E122A0z  0x61DFC6CCz 0x61DFCF94z 0x61DFF270z
  0x61DFC5F8z 0x61E980E0z   %SYS-2-WATCHDOG: Process aborted on watchdog timeout,
  process = SSH Process.
  ```

Conditions: This issue occurs when there the response from the client is slow.

Workaround: Close the connection.

- CSCtr45287

  Symptoms: Router crashes in a scale DVTI scenario.

  Conditions: The symptom is observed when the IPsec tunnel count reaches around 2500.

  Workaround: Use fewer tunnels or use a different platform.

- CSCts54641

  Symptoms: Various small, medium, or big VB chunk leaks are seen when polling EIGRP MIB or during SSO.

  Conditions: This symptom is observed when MIBs are being polled or SSO is done.

  Workaround: There is no workaround.

- CSCtu28696

  Symptom: The Cisco ASR 1000 router crashes at rip_process_mgd_timers decode.

  Conditions: This issue occurs when 500 6rd tunnel and rip are configured, traffic is started and then stopped, and configuration is cleared.

  Workaround: There is no workaround.

- CSCtw88689

  Symptoms: A crash is seen while applying the 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.

- CSCtx54882

  Symptoms: A Cisco ASR 1000 router may crash due to Bus error crash at voip_rtp_is_media_service_pak.

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 15.1(4)M2.

  Workaround: There is no known workaround.

- CSCtx75190

  Symptom: 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 issue occurs with scaled OTV config in a multihomed setup do a RP switchover.

  Workaround: There is no workaround.

- CSCtx80535

  Symptoms: DHCP pool that is configured for ODAP assigns the same IP to multiple sessions.

  Conditions: PPP users receive pool via Radius. The pool is defined on the Cisco 10000 series router to use ODAP. ODAP is receiving the subnets from Radius correctly, and assigns IPs to PPP sessions, but sometimes two users end up having the same IP address.

  Workaround: Clear both sessions sharing the same IP.

- CSCty12312

Symptoms: Multilink member links move to an up/ down state and remain in this condition.

Conditions: This symptom occurs after multilink traffic stops flowing.

Workaround: Remove and restore the multilink configuration.

- CSCty35726

  Symptoms: The following message is displayed in the logs:

  ```
  InterOp:Cube-NavTel : LTI: Video Xcode Call with plain Audio FAILS
  ```

  Conditions: This symptom is seen when video Xcode call with plain audio fails.

  Workaround: There is no workaround.

- CSCty64255

  Symptoms: 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: Hard-clearing the BGP resolves the issue.

- CSCty86039

  Symptoms: Shut down the physical interface of tunnel source interface. The router crashes with traffic going through some of the tunnels.

  Conditions: This symptom is seen with tunnel interface with QoS policy installed.

  Workaround: There is no workaround.

- CSCty89224

  Symptom: IOS router may crash under certain circumstances when receiving a mvpnv6 update.

  Conditions: This issue occurs while receiving a mvpnv6 update

  Workaround: There is no workaround.

- CSCtz37164

  Symptoms: The requests to the RADIUS server are retransmitted even though the session no longer exists, causing unnecessary traffic to RADIUS, and RADIUS getting requests for an invalid session.

  Conditions: This symptom occurs when the RADIUS server is unreachable and the CPE times out the session.

  Workaround: This issue can be avoided by making sure that the RADIUS server is always reachable.

- CSCtz44989

  Symptoms: An EIGRP IPv6 route redistributed to BGP VRF green is not exported to VRF RED. Extranet case is broken for IPv6 redistributed routes.

  Conditions: The issue is seen with IPv6 link-local nexthop. When the EIGRP route is redistributed to BGP VRF, it clears the nexthop information (it become 0.0.0.0). Now this route becomes invalid and BGP is not able to export to another VRF.

  Workaround: There is no workaround.

- CSCtz48338

  Symptom: A Cisco ASR 1000 router may crash.

  Conditions: This issue is observed in a setup with configuration of BGP L3VPN VRF to global export, NSR, and large scale, hard clear or link flap.

Workaround: There is no workaround.

- CSCtz50204

  Symptoms: A crash is observed on EzVPN Server if VRF configuration under the ISAKMP profile is modified.

  Conditions: The crash is observed only if there are active sessions at the time of configuration change.

  Workaround: Prior to applying a configuration change, clear the sessions.

- CSCtz58941

  Symptoms: The router crashes when users execute the **show ip route XXXX** command.

  Conditions: This symptom is observed during the display of the **show ip route XXXX**, when the next-hops of "XXXX" networks are removed.

  Workaround: The **show ip route XXXX** command (without "XXXX") does not have the problem.

- CSCtz61556

  Symptoms: ATM local switching segments do not come up after changing encap on both interfaces.

  Conditions: This symptom is seen with ATM VC local switching. If the encap on both the ATM VC segments are changed, the segments remain in DOWN state.

  Workaround: There is no workaround.

- CSCtz71084

  Symptoms: When the prefix from CE is lost, the related route that was advertised as best-external to RR by PE does not get withdrawn. Even though the BGP table gets updated correctly at PE, RIB still has a stale route.

  Conditions: This symptom is observed with a topology like shown below, where CE0 and CE1 advertise the same prefixes.

  Workaround: Hard-clearing the device solves this issue.

- CSCtz83221

  Symptoms: Active or standby route processor crashes.

  Conditions: This symptom can be seen during the configuration or removal of ATM virtual circuits.

  Workaround: There is no workaround.

- CSCtz92606

  Symptoms: MFR memberlinks-T1 serial interfaces created under a CHOC12 controller, do not get decoupled from MFR even after the MFR bundle interface is deleted. Once the MFR bundle interface is reconfigured, the memberlinks do not appear under it.

  Conditions: This symptom is seen with MFR with memberlinks as T1 serials from CHOC12 sonet controller.

  Workaround: Unconfigure and reconfigure the encap frame-relay MFRx under each memberlink after reconfiguring the MFR bundle interface.

- CSCtz94902

  Symptom: Memory allocation failure occurs.

  Conditions: This issue occurs while attaching to SIP-40 using a web browser.

  Workaround: Reset the line card.

- CSCtz96504

Symptom: Some of the backup VCs are down after SSO.

Conditions: It happens only on scale scenario, in this bug submitter created 500 primary and 500 backup VCs

Workaround: These backup VCs can be brought to SB state by issuing the following command although it is not usually recommended, it is only way to recover: **clear xconnect peerid** <*peerid of the PW*> **vcid** <*vcid*>.

- CSCua06598

  Symptoms: Router may crash with breakpoint exception.

  Conditions: The symptom is observed when SNMP polls IPv6 MIB inetCidrRouteEntry and there is a locally-sourced BGP route installed in IPv6 RIB.

  Workaround: Disable SNMP IPv6 polling.

- CSCua13322

  Symptom: Routes for the converted dedicated P sessions are missing after a RP switchover.

  Conditions: Converted dedicated IP sessions are not HA aware. Therefore after a 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.

- CSCua18542

  Symptoms: When service change occur as ISG, in some particular conditions, the SCE is not ready to accept the CoA, In that case the ISG resends an Update Session on the ISG-SCE Bus. The Update Session is sent but it is not populated with the required attribute for SCE (policy, service-monitor)

  Conditions: There are no specific conditions for the occurrence of this symptom.

  Workaround: There is no workaround.

- CSCua19425

  Symptoms: RP crashes at the far end, pointing to Watchdog Process BGP.

  Conditions: This symptom is observed when doing an FP reload at the near end. This issue is seen with EBGP sessions with BFD configured between near end and far end routers.

  Workaround: There is no workaround.

- CSCua21166

  Symptoms: IPSec tunnels fail to be formed due to error: "RM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with securityk9 technology package license."

  Conditions: Even though the router does not have 225 IPsec SA pairs, error will prevent IPSec from forming. Existing IPSec SAs will not be affected.

  Workaround: Reboot to clear out the leaked counter, or install hsec9 which will disable CERM (Crypto Export Restrictions Manager).

- CSCua21201

  Symptom: RP2 gets reloaded.

  Conditions: This issue occurs when one dynamic crypto map with 8k tunnels running 700Mbps 64B packets are processed.

  Workaround: There is no workaround.

- CSCua27852

Symptoms: Traffic loss is seen in pure BGP NSR peering environment.

Conditions: The 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.

- CSCua28346

  Symptoms: A router crashes during second rekey.

  Conditions: This symptom occurs with IKEv2 with RSA authentication.

  Workaround: There is no workaround.

- CSCua30053

  Symptoms: Authentication fails for clients after some time because the radius_send_pkt fails, because it complains about the low IOMEM condition.

  Conditions: In AAA, minimum IO memory must be 512KB to process the new request. If the memory is less than this, AAA does not process the new authentication request. This is AAA application threshold. This application barriers are not valid in dynamic memory case. Such conditions are removed for NG3K platform.

  Workaround: There is no workaround.

- CSCua33821

  Symptoms: CPU utilization shoots up to 99% after configuring crypto maps.

  Conditions: The symptom is observed after applying crypto maps.

  Workaround: There is no workaround.

- CSCua34638

  Symptoms: A crash is seen on RP2, when the **show platform software shell command package** command is issued.

  Conditions: This symptom is observed when the **show platform software shell command package** command is issued. It impacts the RP2 (x86_64_*) image only.

  Workaround: There is no workaround. Do not issue the **show platform software shell command package** command.

- CSCua35235

  Symptoms: Trace route for TP does not work as expected.

  Conditions: This symptom occurs with a TP setup.

  Workaround: There is no workaround.

- CSCua37898

  Symptoms: Memory leaks are observed.

  Conditions: The memory leaks are seen when OSPFv3 authentication is enabled over virtual link, and the OSPFv3 process is restarted.

  Workaround: There is no workaround.

- CSCua39107

  Symptoms: In a FlexVPN Spoke to Spoke setup, Resolution reply goes via the Tunnel interface to the Hub.

Conditions: This symptom is only observed when NHO is added for the V-Access, overriding an existing route. This issue is not seen when H route is added.

Workaround: Distribute the summarized address from the Hub, thus avoiding addition of NHO at the Spokes. The Spokes will then add H route instead of NHO.

- CSCua40790

  Symptoms: Memory leaks occur when SNMP polling cbgpPeer2Entry MIB.

  Conditions: This symptom occurs when BGPv4 neighbors are configured.

  Workaround: There is no workaround if this MIB is to be polled.

- CSCua41398

  Symptom: The SUP720 crashes.

  Conditions: This issue occurs when you issue the sh clns interface | i ^[A-Z]|Number of active command multiple times via script with following error and decodes:

```
%ALIGN-1-FATAL: Corrupted program counter 00:53:22 EET Tue Jun 5 2012 pc=0x0 ,
ra=0x411514F4 , sp=0x55A8B080  c7600s72033_rp-adventerprisek9-m.122-33.SRE5.symbols.gz
read in Enter hex value: 0x407F5B70 0x407F612C 0x407E026C 0x42BCA588 0x407EDDFC
0x41A78BB8 0x41A78B9C 0x407F5B70:get_alt_mode(0x407f5b68) 0x8
0x407F612C:get_mode_depth(0x407f6118) 0x14 0x407E026C:parse_cmd(0x407ded18) 0x1554
0x42BCA588:parser_entry(0x42bca360) 0x228 0x407EDDFC:exec(0x407ed344) 0xab8
0x41A78BB8:r4k_process_dispatch(0x41a78b9c) 0x1c
0x41A78B9C:r4k_process_dispatch(0x41a78b9c) 0x0
```

  Workaround: There is no workaround.

- CSCua43930

  Symptoms: Checksum value parsed from GRE header does not populate, causing the GRE tunnel checksum test case to fail.

  Conditions: The issue is seen on a Cisco ISR G2.

  Workaround: There is no workaround.

- CSCua45114

  Symptom: Default sessions do not establish when you apply VRF as a service to the default policy. VRF can only be applied to a default session by assigning a VRF on the access-interface. However with dedicated sessions, one cannot apply a VRF on the access-interface and VRF transfer at the same time. Thus if we require VRF transfer on dedicated sessions, we need VRF transfer on lite sessions as well.

  Conditions: This issue occurs when access-side interface is in the default VRF and VRF is applied as a service to the default policy.

  Workaround: There is no workaround.

- CSCua45122

  Symptoms: Multicast event log preallocated memory space needs to be conserved on the low-end platform.

  Conditions: This symptom is observed with multicast even log.

  Workaround: There is no workaround.

- CSCua45548

  Symptoms: Router crashes when **show ip sla summary** command is run.

Conditions: The symptom is observed on Cisco 2900, Cisco 1900, and Cisco 3945 routers configured with IPSLA operations. The router which was idle for one day crashes on issuing the **show ip sla summary** command.

Workaround: There is no workaround.

- CSCua47570

  Symptoms: The **show ospfv3 event** command causes the router to crash.

  Conditions: The symptom is observed when "ipv4 address family" is configured and redistribution into OSPFv3 from other routing protocols is configured.

  Workaround: Do not use the **show ospfv3 event** command.

- CSCua50961

  Symptom: In the Pseudowire redundancy, secondary Pseudowire fails to come up that is also configured as the backup on the other side.

  Conditions: In the Pseudowire redundancy, cannot bring up the secondary Pseudowire that is also configured as the backup on the other side. There are no issues in activating pseduwires that are primary on the other side.

  Workaround: Terminate these pseudowires on a different AC and make them as primary. If the customer want to terminate on the same AC, there is no work around.

- CSCua51991

  Symptoms: An invalid SPI message is seen throughout the lifetime of IPsec SA.

  Conditions: This symptom is observed with SVTI-SVTI with a GRE IPv6 configuration. When bringing up Cisco ASR 1000 Series router sessions, an invalid SPI is seen. There is also inconsistency between the number of child SAs in IKEv2 and the number of IPsec SAs on the same box.

  Workaround: There is no workaround.

- CSCua55691

  Symptoms: A Cisco IOS memory leak is observed.

  Conditions: This symptom is seen when unconfiguring/reconfiguring BGP AD VFIs.

  Workaround: There is no workaround.

- CSCua56184

  Symptom: Flexvpn server crashes after overnight RP switchovers in ASR1000.

  Conditions: Multiple RP switchovers in ASR1000 and it fails to allocate an IPsec SPI.

  Workaround: There is no workaround.

- CSCua56209

  Symptom: PWs does not come up 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. This is a very corner case and the chance of happening in the real deployment scenarios is very low.

  Workaround: Run the **clear xconnect all command** to bring up the PWs.

- CSCua56802

  Symptoms: QoS do not work on one of the subinterfaces/EVC.

Conditions: This symptom occurs when HQoS policy is configured on more than one subinterface/ EVC on ES and then add flat SG on them.

Workaround: Remove and reapply SG.

- CSCua61814

  Symptom: Overhead accounting configuration changes on XE37 image.

  Conditions: This issue occurs in the following conditions:

  - XE34: overhead accounting configure at parent only XE35: overhead accounting configure at parent only
  - XE37: overhead accounting need to be configured on both parent and child policy

  Workaround: There is no workaround.

- CSCua63182

  Symptom: Incorrect minimum bandwidth displayed when a 0k packet is received.

  Conditions: Different behavior in ASR code when Min BW of 0 Kbit is received. 2.6.2 uses 10 Gbps as Min BW in case Min BW = 0 received 3.4.3 uses 1 Kbit as Min BW in case Min BW = 0 received

  Workaround: There is no workaround.

- CSCua67998

  Symptoms: System crashes.

  Conditions: This symptom occurs after adding or removing a policy-map to a scaled GRE tunnel configuration.

  Workaround: There is no workaround.

- CSCua69657

  Symptoms: Traceback is seen when the **show clock detail** command is executed.

  Conditions: This symptom is seen when executing the **show clock detail** command with Cisco IOS interim Release 15.3(0.4)T.

  Workaround: There is no workaround.

- CSCua70065

  Symptoms: CUBE reloads on testing DO-EO secure video call over CUBE when SDP passthru is enabled.

  Conditions: The symptom is observed when running Cisco IOS interim Release 15.3(0.4)T.

  Workaround: There is no workaround.

- CSCua71038

  Symptoms: Router crashes.

  Conditions: The symptom is observed with a Cisco router that is running Cisco IOS Release 15.2(3)T1. The router may crash during the failover test with OCSP and CRL configured.

  Workaround: Configure OCSP or CRL but not both.

- CSCua78782

  Symptoms: Authentication of EzVPN fails.

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

  Workaround: There is no workaround.

- CSCua80204

Symptoms: 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.

- CSCua84879

  Symptoms: Crash at slaVideoOperationPrint_ios.

  Conditions: The symptom is observed when IPSLA video operations are configured and **show running-config** is issued.

  Workaround: There is no workaround.

- CSCua84923

  Symptoms: Following a misconfiguration on a two-level hierarchical policy with a user-defied queue-limit on a child policy, the UUT fails to attach the QoS policy on the interface even when corrected queueing features are used.

  Conditions: This symptom is observed with the following conditions: 1) The issue must have the user-defined queueu-limit defined. 2) This error recovery defected is confirmed as a side effect with the c3pl cnh component project due to ppcp/cce infrastructure enhancement.

  Workaround: There is no workaround.

- CSCua85934

  Symptoms: 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 with the ISG-SCE interface.

  Workaround: There is no workaround.

- CSCua86310

  Symptoms: When relay is configured with 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 happens only when unnumbered loopback address is used on the relay interface which connects to server. If an IPv6 address is used directly on the interface, it works fine.

  Workaround: Use numbered interface instead of unnumbered interface.

- CSCua87944

  Symptoms: In an IPv6 snooping policy, the keyword "prefix-list" has no effect on control packet. The keyword only affects the binding table recovery. In an "ipv6 nd raguard" policy, the limited-broadcast keyword appears though 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.

- CSCua91104

  Symptoms: ISIS adjacency process shows traceback messaging related to managed timer.

  Conditions: This symptom is seen when configuring isis network point-to-point on LAN interface with isis bfd or isis ipv6 bfd enabled. The traceback does not happen always. 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.

- CSCua93136

  Symptoms: The switch crashes when sending the DHCPv6 packet with "ipv6 snooping" on VLAN configurations.

  Conditions: This symptom occurs when sending the DHCPv6 packet with "ipv6 snooping" configured on VLAN configurations.

  Workaround: There is no workaround.

- CSCua94947

  Symptoms: RP crashes when downloading FreeRadius Framed-IPv6-Route on MLPPP sessions.

  Conditions: This symptom occurs when downloading radius Framed-IPv6-Route.

  Workaround: There is no workaround.

- CSCub07382

  Symptom: NHRP cache entry for the spokes get deleted on NHRP timer expiry even though there is traffic flowing through the spoke to spoke tunnel.

  Conditions: This issue occurs on FlexVPN Spoke to Spoke setup.

  Workaround: Configure the same hold time on both Tunnel interface and the Virtual-Template interface.

- CSCub07673

  Symptoms: IPsec session does not come up for spa-ipsec-2g if ws-ipsec3 is also present. "Volume rekey" is disabled.

  Conditions: This symptom occurs if "volume rekey" is disabled.

  Workaround: Do not disable the volume rekey.

- CSCub09124

  Symptoms: MDT tunnel is down.

  Conditions: This symptom is seen in MVPN. If the **ip multicast boundary** command on non-current RPF interface blocks the MDT group, it may cause MDT tunnel failure.

  Workaround: Adding the **static join** command under PE loopback interface may work around the problem temporarily.

- CSCub15542

  Symptoms: Configuring mpls lsp trace results in IOSD restart.

  Conditions: This symptom occurs when configuring mpls lsp trace results in IOSD restart.

  Workaround: There is no workaround.

- CSCub17985

  Symptoms: 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 a part of the subscriber profile. On applying these routes to the sessions, a memory leak is observed.

  Workaround: There is no workaround.

- CSCub21340

  Symptom: Segmentation fault crash and router reloads continuously.

  Conditions: When router is reloaded with cfm over xconnect scale config (configuring 500 meps)

  Workaround: There is no workaround.

- CSCub24355

  Symptoms: IPv4 mVPN inactive (S,G) are not removed on egress PE.

  Conditions: There are no specific conditions for the occurrence of this symptom.

  Workaround: Remove entries manually.

- CSCub32500

  Symptom: Router crashes in EIGRP due to chunk corruption.

  Conditions: This issue is seen on EIGRP flaps.

  Workaround: There is no workaround.

- CSCub33877

  Symptom: During the "issue loadversion", while downgrading from Texel (or later) to Yap (v151_1_sg_throttle or earlier), the standby RP keeps reloading due to the out of the sync of configuration.

  Conditions: The issue occurs during issu loadversion operation. The newer version of image supports the ipv6 multicast while the older version of image does not.

  Workaround: There is no workaround.

- CSCub42920

  Symptom: KS rejects rekey ACK from GM with message (from "debug crypto gdoi ks rekey all"): GDOI:KS REKEY:ERR:(get:0):Hash comparison for rekey ack failed. The keys & policies in the rekey packet are correctly installed by the GM, but the rekey ACK does not get processed by the KS. This leads to rekey retransmissions, GM re-registration and potential disruption of communication.

  Conditions: Rekey ACK validation in versions 15.2(4)M1 (ISR-G2) and 15.2(4)S/3.7S (ASR1000) is incompatible with other software releases. A KS that runs 15.2(4)M1 or 15.2(4)S/3.7S will only be able to perform successful unicast rekeys with a GM that runs one of those two versions. Likewise, a KS that runs another version will only interoperate with a GM that also runs another version.

  Workaround: Use multicast rekeys.

- CSCub46570

  Symptoms: The image cannot be built with an undefined symbol.

  Conditions: This symptom occurs as the commit error triggers the compiling issue.

  Workaround: There is no workaround.

- CSCub49291

  Symptom: Static tunnels between hubs and spokes fails to rebuild.

  Conditions: Reload hub on the DMVPN ipv6 setup with DPD on-demand enabled on all spokes.

  Workaround: There is no workaround.

- CSCub54872

  Symptom: A /32 prefix applied to an interface (for example, a loopback) is not being treated as connected. This can then prevent Half-Duplex VRFs for operating correctly.

  Conditions: This issue occurs when the prefix is applied to an interface is for a host route (/32 for Ipv4 or /128 for IPv6).

  Workaround: Use a shorter prefix.

- CSCub67101

Symptoms: The POS interface line protocol is 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. Then, the interface will come up in the proper state.

- CSCub73159

  Symptom: IOSD crashes.

  Conditions: This issue occurs while bringing up 8k PPP sessions with QOS and ebgp routes.

  Workaround: There is no workaround.

- CSCub73430

  Symptom: A Cisco ASR 1000 Series Aggregation router running IOS 15.2.(4)S ipBaseK9 feature set crashes when a interface that a qos policy attached to it comes up.

  Conditions: This issue occurs on an interface with a qos policy attached.

  Workaround: Use other feature sets, AdvEnterpriseK9, for example.

- CSCub81374

  Symptom: A Cisco ASR1001 router Feature Navigator does not show correct image to license mapping.

  Conditions: This issue occurs on a Cisco ASR1001 router with or without licenses.

  Workaround: There is no workaround.

- CSCub96074

  Symptom: Software is forced to reload on a Cisco ASR 1000 Series Aggregation Router using the ISG feature.

  Conditions: ISG sessions cannot be authenticated/authorized whenever primary/secondary Radius servers are marked as unreachable. This creates high load on ISG and may force a crash.

  Workaround: There is no workaround.

- CSCub96743

  Symptom: Packet drops are seen on Scaled Cisco ASR 1000 Series Aggregation Router during RP switchover.

  Conditions: This issue occurs during RP and FP switchover.

  Workaround: There is no workaround.

- CSCub99756

  Symptom: A Cisco ASR 1000 router running 15.2(4)S release acting as a GM in a GETVPN deployment starts using the most recent IPSEC sa upon KS rekey instead of using the old key up to 30 seconds of expiration.

  Conditions: This issue was observed only in 15.2.(4)S.

  Workaround: There is no workaround.

- CSCub99778

  Symptom: A Cisco ASR 1000 router being GM in a GETVPN deployment fails to start GDOI registration after a reload. The following status is seen: Registration status : Not initialized in the show crypto gdoi output after a reload.

  Conditions: This issue occurs while running 15.2(4)S.

Workaround: Use an EEM script to issue a "clear crypto gdoi" a bit after boot time or issue this manually.

- CSCuc15548

  Symptom: Subscriber session on LAC/LNS attempts state with "vpdn authen-before-forward"cli configured and auto-service in the radius-profile.

  Conditions: This issue occurs because of the command "vpdn authen-before-forward" and one auto-service in the user's profile in radius.

  Workaround: Configure and apply one policy-map with SESSION-START rule with at least one action.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7S

This section describes the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7S. It contains the following topic:

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7S

This section documents the unexpected behavior that might be seen in Cisco ASR 1000 Series Aggregation Services Routers Release 3.7S.

- CSCtx89616

  Symptom: BITS e1 output network-clock source configuration sends QL-INV to remote end.

  Conditions: This issue is observed when the configuration of BITS e1 output network-clock source sends QL-INV to the remote end.

  Workaround: There is no workaround.

- CSCty21018

  Symptom: Occasionally, network boots from ROMMON may run very slowly. Booting from a "tftp:" device may appear to stall or run very slowly.

  Conditions: This issues is observed when attempting to boot from a "tftp:" device.

  Workaround: In non-autoboot scenarios, where the console port is connected, issue a **reset** under user supervision.

  If the system is configured to autoboot, reconfigure the TFTP_TIMEOUT environment variable from its present very long value to a value longer than the expected boot time considering the network and server load. If the system finds itself in this slow booting mode while autobooting, the transfer will time out, and autoboot will reset and attempt to netboot the file again.

  A suggested starting value of 300 seconds can be provided from the ROMMON prompt:

```
TFTP_TIMEOUT=300
Sync
```

- CSCtz74060

  Symptom: The output of **show platform hardware qfp active feature ess state** command is not working and is showed in XML format during ISSU sub-pkg downgrade from XE3.7.0 to lower releases on 4RU. There is no functionality impact.

  Conditions: This issue is observed during ISSU upgrade process with ESP and RP running at different versions. There is no functional impact with this issue. The command work correctly after the system upgrade is complete.

  Workaround: There is no workaround.

- CSCua71731

  Symptom: When configuring the maximum throughput on a Cisco ASR 1002-X router, a value of 40000000 kbps is indicated even though the actual limit is 36000000 kpbs. Several log messages also indicates a value as 40000000 kbps when the license changes or is rejected. Actual product license or throughput is not affected.

  Conditions: This issue is observed in the configuration mode. Log messages would vary dependent on action. But the output include message similar to the following message:

  ```
  "*Aug 14 21:42:30.294: %IOSXE_THROUGHPUT-3-INVALID_CONFIG: No valid license found for
  the configured throughput level: 40000000 kbps"
  ```

  Workaround: There is no workaround.

- CSCtx81748

  Symptom: A small amount of packet drop due to anti-replay failure may be seen when the IPSec feature is configured.

  Conditions: This issue is observed when the IPsec session is starting or when the IPSec SA lifetime expires and a new SA is established.

  Workaround: There is no workaround.

- CSCty55408

  Symptom: Pending issues and acknowledgments are observed after unconfiguring and configuring the same scale configuration while traffic is flowing.

  Conditions: This issue is observed when four overlays are configured with 500 EFPs per overlay. Remove the overlay and EFP configuration. Copy the same configuration back on one of the routers.

  Workaround: There is no workaround.

- CSCtz24454

  Symptom: POS interfaces are stuck in down state.

  Conditions: This issue is observed while reloading a Cisco ASR1000 or a SPA.

  Workaround: Reload the FP.

- CSCtz34089

  Symptom: Cisco ASR1000 devices displays traceback after RP switchover.

  Conditions: This issue is observed with DMVPN HUB when scaled to 4000 spokes.

  Workaround: There is no workaround.

- CSCtz69971

  Symptom: High IPSec/QoS latency.

  Conditions: This issue is observed when traffic with volume-based rekey is sent.

Workaround: There is no workaround.

- CSCtz71147

  Symptom: IPv6 IPSec tunnel start up may be slow and pending objects may be seen in the **show platform software object-manager fp active statistics** command output.

  Conditions: This issue is observed when trying to start large number of IPv6 tunnels (500 tunnels or more) after configuring them.

  Workaround: There is no workaround.

- CSCtz74060

  Symptom: The CLI output format of the **show platform hardware qfp active feature ess state** command has changed.

  Conditions: This issue was observed during ISSU sub-pkg downgrade from XE3.7.0 to lower releases on 4RU while FP is running XE3.7.0 image and Active RP is running non-XE3.7.0 images.

  Workaround: There is no workaround.

- CSCua08206

  Symptom: VCs configured with VPLS on the standby RP is in down state.

  Conditions: This issue is observed during a core link flap.

  Workaround: Clear xcon all.

- CSCua18917

  Symptom: End to End Traffic fails in Port-channel QinQ Xconnect circuit.

  Conditions: This issue is observed in a scaled configuration of 100 Port-channel subinterfaces configured using a script.

  Workaround: Reload the router.

- CSCua30168

  Symptom: IOSd restarts.

  Conditions: This issue is observed during a mixed tunnel scaling test with high traffic.

  Workaround: There is no workaround.

- CSCua40578

  Symptom: mGREv6:IPv6 NHRP Shortcut switching not working for IPv6 transport.

  Conditions: This issue is observed on a topology with two spokes registered to a Hub. Tunnel interfaces in mGREv6 mode is configured on bob and spokes and NHRP shortcut and redirect switching is configured on the tunnel interfaces.

  Workaround: There is no workaround.

- CSCua49474

  Symptom: TCP segments of specific length may be forwarded with wrong packet payload if the NAT feature is configured on Cisco ASR 1000 Series Aggregation Services Routers.

  Conditions: This issue is observed when NAT is configured on the device and the TCP segments are of specific length.

  Workaround: There is no workaround.

- CSCua55495

  Symptom: BGP entries fail to return to the original value within 600 seconds.

Conditions: This issue is observed on DMVPN networks.

Workaround: There is no workaround.

- CSCua59573

  Symptom: CPP crashes after modifying scaled VPLS configuration and changing the loop back address.

  Conditions: This issue is observed only in scaled VPLS setup and on doing a negative test by changing the loop back address.

  Workaround: There is no workaround.

- CSCua69725

  Symptom: Pending objects and traffic loss.

  Conditions: This issue is observed on cell packed interfaces.

  Workaround: Reload the router.

- CSCua75088

  Symptom: The OSPF relationship between PE & P routers disappears after reloading carrier card several times.

  Conditions: This issue is observed if the carrier card is reloaded multiple times.

  Workaround: There is no workaround.

- CSCua77720

  Symptom: cpp_svr restarts on an optimised edge router (OER) border router.

  Conditions: This issue is observed during a tunnel flap on external interfaces or while replacing a configuration.

  Workaround: There is no workaround.

- CSCua81608

  Symptom: IOSd crashes and router reloads multiple times after the ISSU upgrade.

  Conditions: This issue is observed while running 4RURP1 ISSU sub package forwarding with all features from Cisco IOS XE 3.5.2 and Cisco IOS XE 3.6.

  Workaround: There is no workaround.

- CSCua87736

  Symptom: End to End ping and Traffic Fails.

  Conditions: This issue is observed on IP internetworking with port-channel Xconnect QINQ ANY encapsulation.

  Workaround: There is no workaround.

- CSCua87896

  Symptom: qfp exmem is exhausted on the standby FP.

  Conditions: This issue is observed when TCP is used for SIP signalling.

  Workaround: There is no workaround.

- CSCub01576

  Symptom: The ESP reloads on a Cisco ASR1000 router due to ucode crash.

Conditions: This issue is observed an Cisco ASR1000 router where Layer 4 Redirect feature is configured. This problem was first observed in 15.2(01)S release. This issue may not occur in some customer environments to about once a 1 week in medium sized high CPS ISG production networks.

Workaround: There is no workaround.

- CSCub03744

  Symptom: ESP 100 crashes.

  Conditions: This issue is observed while removing a hierarchical QoS policy-map from a port-channel member link.

  Workaround: There is no workaround.

- CSCub10859

  Symptom: The following symptoms are observed:

  - Cisco ASR 1006 turns unresponsive unexpectedly; even on both console ports.
  - After the router processor is reset, other modules remain down and do not recover.
  - Performing a soft OIR on failed modules does not work.
  - After the SIP is reset, the interfaces remain down and you need to run shut and no shut commands to restart the interfaces.
  - No coredump or crashinfo is generated.
  - One power supply shows zero volt.

  Conditions: This issue is observed on only on two Cisco ASR 1006 devices with 2x RP2, 2x ESP40, SIP40 and 2x ASR1013/06-PWR-DC

  Workaround: Power cycle the chassis.

- CSCua13561

  Symptom: Clients fail to get the IP address through the PPP IPCP from DHCP pool.

  Conditions: This issue occurs after upgrading a Cisco ASR 1000 Series Aggregation Services Router from Cisco IOS XE 12.2(33) XNF2 to Cisco IOS XE 15.2(2)S without any configuration changes.

  Workaround: There is no workaround.

- CSCua26487

  Symptom: The SNMP loops at OID 1.3.6.1.4.1.9.9.645.1.2.1.1.1, and as a consequence, the SNMP walk fails.

  Conditions: This issue is observed only during an SNMP getbulk request on OID 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. For details on excluding the MIB table from the SNMP walk, see the following configurations:

  ```
  snmp-server view <view name> iso included
  snmp-server view <view name> ceeSubInterfaceTable excluded
  snmp-server community <community> view <view name>
  ```

- CSCua40273

  Symptom: The Cisco ASR 1000 Series Aggregation Services Router crashes when displaying MPLS VPN MIB information.

  Conditions: This issue occurs on the Cisco ASR 1000 Series Aggregation Services Routers running IOS XE 15.1(02)S.

Workaround: Avoid changing the VRF while querying for MIB information.

- CSCua58100

  Symptom: The syslog is flooded with traceback message similar to the following 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: This issue occurs under the following conditions:

  - You establish 36 k EAPSIM sessions using a RADIUS client on server A.
  - You establish 36 k roaming sessions using a RADIUS client on server B.
  - The roaming sessions have the same caller-station-id but use an IP address that is different from the EAPSIM sessions.

  Workaround: There is no workaround.

- CSCtw72855

  Symptom: The router does not pass traffic towards the access side on the VCs configured with QoS shaping output policy.

  Conditions: This issue occurs when you configure a QoS shaping output policy.

  Workaround: There is no workaround.

- CSCty28986

  Symptom: A configuration with a high number of down MEPs does not function properly.

  Conditions: This issue occurs when you configure 500 or more down MEPs with 500 or more Xconnect configurations between service instances.

  Workaround: Configure no more than 200 CFM sessions.

- CSCty34054

  Symptom: The router displays CPU utilization traceback messages and drops all multicast traffic for 2050 seconds.

  Conditions: This issue occurs under the following conditions:

  - Multicast is enabled with more than 500 multicast groups.
  - The router is using RSP1B in SSM mode.
  - BDI is configured on the access side of the router.
  - There are 24 EFPs on each bridge domain.
  - You enter a **shutdown** command on the access interface.

  Workaround: There is no workaround.

- CSCty51990

  Symptom: The router may crash or restart, with the console displaying a **`SW_WDOG: expired`** message.

  Conditions: This issue occurs under the following conditions:

  - The router is configured with 63 or more instances of a unique EVC configured with a unique BDI.
  - The router is sending IGMP joins to one multicast group.

- You perform a shutdown or no shutdown on the interface sending IGMP join messages.
- You perform an OIR on the router.

Workaround: There is no workaround.

- CSCty70119

  Symptom: Port shaper rate changes do not take effect.

  Conditions: This issue occurs when QoS policies attached to EVCs on an interface do not include a shaper configuration; issue does not occur on EFP policies that include a shaper in a class.

  Workaround: Include a shaper in one class of EFP policies.

- CSCty73362

  Symptom: The router experiences CPP download failures when sending IGMP join messages.

  Conditions: This issue occurs when the router is configured with a trunk EFP in SM mode on the access side, and is sending IGMP join messages to more than 1970 multicast groups.

  Workaround: There is no workaround.

- CSCty74115

  Symptom: The router displays traceback and CPU error messages.

  Conditions: This issue occurs when you configure a large number of MAC address table entries while REP is enabled. The router displays errors during an REP topology change, REP pre-emption, or when you perform a shutdown/no shutdown on an interface.

  Workaround: Reduce the MAC scale.

- CSCty79987

  Symptom: The Connectivity Fault Management (CFM) up Maintenance End Points (MEPs) and down MEPs fails to scale to 1000 CFM sessions.

  Conditions: This issue occurs when you configure CFM on a trunk Ethernet Flow Point (EFP).

  Workaround: There is no workaround.

- CSCtz20087

  Symptom: The router applies the class-default QoS policy to all outgoing traffic.

  Conditions: This issue occurs under the following conditions:

  - You configure multiple egress QoS policies on a Gigabit Ethernet interface.
  - You configure a multilink interface with no ingress QoS policy.

  Workaround: There is no workaround.

- CSCtz32327

  Symptom: The router crashes.

  Conditions: This issue occurs when you have an OC-3 IM installed, and perform a soft OIR or SSO (when HA is configured).

  Workaround: There is no workaround; reload the router.

- CSCtz40690

  Symptom: Traceroute to a remote MEP fails.

  Conditions: This issue occurs under the following conditions:

  - You configure a EVC bridge domain MEP on a remote device.

- You configure a MIP on a trunk EFP on an intermediate device.
- You issue the **traceroute** command to the remote MEP.

Workaround: There is no workaround.

- CSCtz49927

  Symptom: Traffic floods an EFP interface.

  Conditions: This issue occurs when you configure a multicast static MAC on a bridge domain and add more than 24 EFPs.

  Workaround: Remove the extra EFPs from the bridge domain.

- CSCtz55979

  Symptom: The router crashes.

  Conditions: This issue occurs when you configure CFM, SCE over MPLS, VPLS, or G.8032 services while running SNMP polling.

  Workaround: There is no workaround.

- CSCtz77491

  Symptom: The router stops passing traffic and crashes.

  Conditions: This issue occurs when you remove a QoS policy applied to a trunk EFP.

  Workaround: There is no workaround.

- CSCtz82725

  Symptom: The router intermittently drops packets.

  Conditions: This issue occurs on 10-Gigabit Ethernet core links when the router passes traffic for an extended period while running a VPLS-TP configuration.

  Workaround: There is no workaround.

- CSCtz87262

  Symptom: The router's convergence time is greater than 90 seconds when you clear the multicast routing table.

  Conditions: This issue occurs with a ring topology with two parallel paths from the FHR to the LHR receivers.

  Workaround: There is no workaround.

- CSCtz90273

  Symptom: The router duplicates multicast traffic when configured as a static rendezvous point (RP) node.

  Conditions: This issue occurs under either of the following conditions:

  - You remove Auto RP announce configurations on all the routers.
  - You configure the router as a static RP and enable multicast traffic.

  Workaround: Select an RP mode: static, auto, or bootstrap router (BSR) and avoid switching dynamically between RP modes.

- CSCtz92857

  Symptom: MAC learning fails and the router displays FIFO table overflow messages.

  Conditions: This issue occurs with a MAC security configuration running at high scale.

Workaround: There is no workaround.

- CSCtz92914

  Symptom: L3 multicast replication fails on some of the EFPs.

  Conditions: This issue occurs under the following conditions:

  - You configure a group of EFPs and map each EVC to a different bridge domain.
  - You create a QoS policy map on each EVC.
  - All the BDI send IGMP joins to a single multicast group.
  - The router initiates multicast data traffic.
  - You remove and reconfigure some of the EFPs.

  Workaround: Configure the EFPs and bridge domains, and initiate the traffic flow before attaching QoS policies.

- CSCua12366

  Symptom: An interface module crashes after an interface module OIR.

  Conditions: This issue occurs when you perform an OIR after the router has been passing traffic for more than 6 hours.

  Workaround: There is no workaround; the IM recovers after the crash and resumes the task of passing traffic.

- CSCua16143

  Symptom: IPv6 BFD sessions drop after you perform an SSO.

  Conditions: This issue occurs when you perform an SSO on the router while running an IPv6 BFD configuration. Note that this issue does not occur with an IPv4 BFD configuration.

  Workaround: After SSO, perform a shutdown and no shutdown on the physical interface.

- CSCua16492

  Symptom: Some IPv6 multihop BFD over BGP sessions flap.

  Conditions: This issue occurs on port channel interfaces running IPv6 multihop BFD over BGP sessions after you perform an SSO.

  Workaround: There is no workaround.

- CSCua33453

  Symptom: A CFM configuration crashes after passing traffic for several hours.

  Conditions: This issue occurs when you create the following configuration:

  - A port channel interface configured with an EVC and applied to a bridge domain.
  - A physical interface configured as a trunk EFP.
  - The **offload** sampling command is configured on both interfaces.

  Workaround: There is no workaround.

- CSCua33788

  Symptom: The router does not pass multicast traffic consistently; only some traffic passes.

  Conditions: This issue occurs when you configure 255 EVCs spanning across different slots on the router.

Workaround: There is no workaround.

- CSCua36065

  Symptom: The router forwards multicast traffic on 63 out of 255 multicast OIFs.

  Conditions: This issue occurs when you configure the following:

  - 255 EVCs on a single port mapped to 255 BDIs (one EVC for each BDI) using rewrite tagging.
  - 255 BDIs that send IGMP v2 Joins to a single multicast group.
  - 255 EVCs configured as a routed ports with the port a member link of a port channel.
  - 255 EVCs configured on a port channel and sending multicast traffic to a multicast group

  Workaround: There is no workaround.

- CSCua38675

  Symptom: The router displays a **`QoS Stats Stalled`** error message and stops applying QoS configurations.

  Conditions: This issue occurs when you apply a flat VLAN policy to a trunk EFP interface.

  Workaround: There is no workaround.

- CSCua41400

  Symptom: QoS classification does not function properly.

  Conditions: This issue occurs when you create QoS class containing a policy that classifies traffic based on both ACLs and DSCP values.

  Workaround: There is no workaround.

- CSCua43843

  Symptom: QoS classification fails when you configure the **match vlan** command under a class map.

  Conditions: This issue occurs when the router is configured with an EVC with the **encapsulation** default command.

  Workaround: Change the encapsulation to dot1q.

- CSCua52162

  Symptom: The router does not learn remote CFM MEPs on an EFP interface.

  Conditions: This issue occurs when you configure rewrite push operation on an EFP interface.

  Workaround: There is no workaround.

- CSCua52187

  Symptom: The router crashes when you attach a QoS policy.

  Conditions: This issue occurs when you apply a QoS class map that:

  - Matches traffic based on an ACL.
  - References an ACL that is not present in the running configuration.
  - Is referenced in a policy with a DSCP marking action.

  Workaround: There is no workaround.

- CSCua54547

  Symptom: The router does not learn remote CFM MEPs.

  Conditions: This issue occurs under the following conditions:

- The router is connected to the remote MEPs via a pseudowire connection.
- The router is configured with MPLS on a bridge-domain interface
- Dot1q encapsulation is configured on an EFP.

Workaround: Configure the EFP encapsulation as untagged.

- CSCua55122

  Symptom: The OC-3 interface module crashes when you create a large number of ATM IMA interfaces.

  Conditions: This issue occurs when you configure multiple ATM IMA interfaces with fewer than 16 links per bundle.

  Workaround: Perform a hard OIR on the interface module.

- CSCua56761

  Symptom: Gigabit Ethernet port 0/5/1 does not timestamp Ethernet OAM Y.1731 packets.

  Conditions: This issue occurs when you configure Ethernet OAM on port 0/5/1 of a copper or SFP Gigabit Ethernet interface module.

  Workaround: There is no workaround.

- CSCua61909

  Symptom: Changes to the **police QoS** command do not take effect.

  Conditions: This issue occurs under the following conditions:

  - You create a QoS policy with a policer and attach the policy to an interface.
  - You make a dynamic change to the police action, such as altering the policer value, the conform-action value, or the exceed-action value.

  Workaround: Remove the policy from the interface, make the necessary changes, and reattach the policy.

- CSCua67795

  Symptom: The router does not transmit Y.1731 Delay Measurement Message (DMM) values using QinQ encapsulation.

  Conditions: This issue occurs with the following configuration:

  - An EFP is configured and applied to a bridge-domain.
  - The EFP is configured with QinQ encapsulation.
  - A Y.1731 Delay Measurement Message (DMM) value is applied.
  - The Y.1731 traffic uses a CoS value other than 0.

  Workaround: There is no workaround.

- CSCua70585

  Symptom: The router does not update the Gigabit Ethernet interface bitmaps after you remove an EFP from a multicast group. However, the router can display CPU hog messages.

  Conditions: This issue occurs under the following conditions:

  - You create an EFP on a single BDI.
  - The router receives IGMP v2 or IGMP v3 SSM joins to the BDI.
  - You create a second EFP on the same BDI.
  - You delete either the first or the second EFP.

Workaround: There is no workaround.

- CSCua72298

  Symptom: The router stops passing traffic on the 10-15 HDLC interfaces.

  Conditions: This issue occurs when you configure a large number of HDLC interfaces: 84 for each port or 336 for each interface module.

  Workaround: Remove and reconfigure the interface.

- CSCua73104

  Symptom: The router does not increment QoS port shaper policy counters displayed by the **show policy interface** command.

  Conditions: This issue occurs when you configure:

  - A class default policy on a physical interface
  - A class-based policy on an EVC interface

  Workaround: There is no workaround. However, the router applies the QoS policy normally.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.7S

This section documents resolved issues on Cisco ASR 1000 Series Aggregation Services Routers Release 3.7S.

- CSCtz47706

  Symptom: IOSD may crash while adding route information for PPP-IP-P2P neighbor (ppp_ip_p2p_neighbor_route_add)

  Conditions: This symptom may occur during session churning of L2TP with BGP.

  Workaround: There is no workaround.

- CSCtx23593

  Symptom: Some virtual circuit (VC) information is missing in the Simple Network Management Protocol (SNMP) MIB object cAal5VccEntry from the output of the snmpwalk router configuration command. For example, The ATM VCs 4/0.120 exist on the router but are missing in the MIB. **Conditions:** This symptom is observed on a Cisco 7204VXR (NPE-G2) router that is running 12.2(33)SRE5 (c7200p-advipservicesk9-mz.122-33.SRE5.bin) image in customer network. The symptom may also occur in other releases.

  Workaround: - Enter the show atm vc privileged EXEC command on the same device to obtain a complete list of all the VCs. OR - Do the SNMPWALK suffixing the ifIndex of the interface to get the value. $ snmpwalk -v 2c -c fwwrcmn na-salerno-ar011 .1.3.6.1.2.1.2.2.1.2 | grep "4/0.120" IF-MIB::ifDescr.253 = STRING: ATM4/0.120-atm subif IF-MIB::ifDescr.254 = STRING: ATM4/0.120-aal5 layer

  $ snmpwalk -v 2c -c fwwrcmn na-salerno-ar011 .1.3.6.1.4.1.9.9.66.1.1.1.1.3 | grep 9.9.66.1.1.1.1.3.254 ===> Got no entry of ifindex here in complete snmpwalk $ $ snmpwalk -v 2c -c fwwrcmn na-salerno-ar011 .1.3.6.1.4.1.9.9.66.1.1.1.1.3.254 ===> When done the SNMPWALK suffixing the ifindex, then getting the value which can be one workaround. SNMPv2-SMI::enterprises.9.9.66.1.1.1.1.3.254.200.106 = Counter32: 403633041

- CSCtz12525

Symptom: Accounting stop send without Acct-Input-Packets Acct-Output-Packets Acct-Input-Octets Acct-Output-Octets when service stop is performed

Conditions: Service stop is issued

Workaround: There is no workaround.

- CSCua24676

  Symptom: VRF to global packet's length corrupted by -1.

  Conditions: Issue seen when the next-hop in vrf is global and recursive going out labeled. Issue is seen from 150-1.S3a onwards not seen on 150-1.S2.

  Workaround: use next hop interface ip instead of recursive next hop.

- CSCua29001

  Symptom: ANCP truncated line rate not seen on standby and hence the policy application will differ from that on active

  Conditions: ancp truncate <value> CLI enabled and port ups received on BRAS

  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 "sh run" can be executed.