Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.9S

This chapter provides information about the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.9S.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.2S

This section describes the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.2S. It contains the following topics:

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.2S

This section documents the unexpected behavior that may be seen in Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.2S.

- CSCue34749

  Symptom: SIP crashes on RP switchover.

  Conditions: Issue is seen in scale setup.

  Workaround: SIP has to be reloaded.

- CSCue91054

  Symptom: ESP crashed when sending IPv6-fragmented traffic through DMVPN hub (MGRE tunnel).

Conditions: This condition occurs when sending big IPv6 packets (need to do IPv6 fragmenation after adding tunnel header) traffic through DMVPN hub. Large amout of IPv6 fragment traffic, for example, 5G on ESP20, which exceeds re-assembly performance number that is less than 2G.

Workaround: Change MTU to avoid IPv6 fragmentation.

- CSCuh18797

  Symptom: ESP crashed while removing policy-map from configuration. This issue is seen while removing the QoS configuration from standalone chassis and all the ports are down.

  Conditions: ESP crashed because of object-pending issue. This issue can only be reproduced when the QoS configuration is from NVRAM, and not when it is added on a live box. This may be related to ordering issue.

  On my 1RU router, just booted the QoS config , and remove the QoS policy will crash FP.

```
QoS-1RU#conf t
Enter configuration commands, one per line. End with CNTL/Z.
QoS-1RU(config)#no policy-map
PM-QOS-LAN-1 QoS-1RU(config)# *May 29 06:31:35 UTC:  IOSXE_OIR-6-OFFLINECARD  Card
(fp) offline in slot F0do *May 29 06:31:46 UTC:  CPPHA-3-FAULT  SIP0: cpp_ha:  CPP:0.0
desc:CPP Client process fail det:HA class:CLIENT_SW sev:FATAL id:1 cppstate:RUNNING
res:UNKNOWN flags:0x0 cdmflags:0x0 *May 29 06:31:46 UTC:  IOSXE-6-PLATFORM  SIP0:
cpp_ha: Shutting down CPP MDM while client(s) still connected *May 29 06:31:46 UTC:
PMAN-3-PROCHOLDDOWN  SIP0: pman.sh:  The process fman_fp_image has been helddown (rc
134) *May 29 06:31:46 UTC:  PMAN-0-PROCFAILCRIT  SIP0: pvp.sh:  A critical process
fman_fp_image has failed (rc 134) *May 29 06:31:46 UTC:  PMAN-3-PROCHOLDDOWN  SIP0:
pman.sh:  The process cpp_ha_top_level_server has been helddown (rc 69) *May 29
06:31:48 UTC:  CPPDRV-3-LOCKDOWN  SIP0: cpp_cp:  CPP10(0) CPP Driver LOCKDOWN due to
fatal error. *May 29 06:31:50 UTC:  IOSXE-6-PLATFORM  SIP0: cpp_cdm: Shutting down CPP
MDM while client(s) still connected *May 29 06:31:52 UTC:  PMAN-5-EXITACTION  SIP0:
pvp.sh:  Process manager is exiting: critical process fault, fman_fp_image, fp_0_0,
rc=134May 29 06:33:03.763 R0/0:  PMAN-5-EXITACTION  Process manager is exiting: reload
fru action requested
```

  Workaround: There is no workaround.

- 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.

- CSCuf74266

  Symptom: ASR-CUBE: Crash observed with DSMP.

  Conditions: Load scenario issue is observed.

  Workaround: There is no workaround.

- CSCug48145

  Symptom: ASR DTMF interworking failed after reinvite with the block configured.

  Conditions: DTMF configured with different preference results in issue.

  Workaround: There is no workaround.

- CSCug77212

  Symptom: ASR1K CUBE RP may crash with Segmentation fault(11), Process = CCSIP_SPI_CONTROL when SIP headers are manipulated using a SIP profile for 200 response messages for KPML notify.

Conditions: Crash could be due to SIP profile configurations being wrongly applied to Notify response (this profile was meant for 200 OK Invite response).

Workaround: Do not configure SIP profiles to manipulate the headers for 200 responses.

- CSCui00417

  Symptom: Linear increase of CPU for CCSIP_SPI_CONTROL and AFW_application processes, and CPU does not stabilize.

  Conditions: Basic SIP calls (INVITE to BYE) run for 2 hours or more.

  Workaround: There is no workaround.

- CSCug19588

  Symptom: IKEv2 TPS performance degradation over time.

  Conditions: This occurs in the lab under extreme test conditions with traffic running during session bring-up.

  Workaround: Reduce traffic and session bring-up rate.

- CSCud78578

  Symptom: RP crashes after FP switchover.

  Conditions: FP(FP80) reload with QoS configurations and traffic flowing in the background.

  Workaround: There is no workaround.

- 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.

- CSCuh73422

  Symptom: ASR1k With MAP-T Configuration crashes.

  Conditions: When a Ping is initiated to public IPv4 address, the Cisco ASR 1000 Series Aggregation Services Routers crash with Core dump, and the packet is translated but the packet causes an ICMP error message to be generated. In case of ICMP error generation, the box could crash.

  Workaround: There is no workaround.

- CSCue14586

  Symptom: After reload, system may not be able to bring up all IPsec tunnels at high scale (1k) group members.

  Conditions: This condition occurs on the Cisco ASR 1000 Series Aggregation Services Routers with GETVPN, 1k group members.

  Workaround: Issue the **clear crypto gdoi** command to force re-registration and rebuild of tunnels.

- CSCue50484

  Symptom: Crypto Tunnel Socket remains OPEN after shutting down the tunnel interface.

  Conditions: This condition occurs on the Dual-DmVPN with ike-profile on the tunnel interface.

  Workaround: There is no workaround.

- CSCuf96673

  Symptom: Memory leaks are seen with Smap-Dmap scale scenario for 4000 sessions.

  Conditions: Leaks are seen after stress testing in **rekey**, **dpd**, and **clear** commands.

Workaround: There is no workaround to prevent memory leaks.

- CSCui21309

  Symptom: ASR RP Crash is observed.

  Conditions: This condition occurs on the Cisco ASR 1002-x Routers running on 3.8.2S. This ASR is configured as dVTI IPSec Server.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCuh56482

  Symptom: A client connects to the IOS headend when launched from the browser, but if the connection attempt is made directly from the client it fails.

  Conditions: This symptom occurs under the following conditions:

  - Cert-only client authentication is configured on the IOS headend.
  - Standalone client is used to connect.
  - There is more than one client certificate on the host machine.

  Workaround: Launch the connection from the browser instead.

- 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.

- CSCui12338

  Symptom: PPPoX sessions are not coming up with scaled configurations above 24,000.

  Conditions: The Service Provider network should be NAT enabled to 200 VRF with MPLS running in the core.

  Workaround: There is no workaround.

- CSCuh92188

  Symptom: Active IOSD crashed because of BGP task, which eventually cause the entire RP to reboot. This issue is not related to BGP task.

  Conditions: This symptom is seen when active IOSD process crashes. The reason of IOSD crash could be anything.

  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.

- CSCue48456

  Symptom: Call is disconnected through CUBE.

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

  Workaround: There is no workaround.

- 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.

- CSCuh95336

  Symptom: Second udpated PDP failed.

  Conditions: Update the second PDP normally with different data TEID.

  Workaround: There is no workaround.

- 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

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.2S

- 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.

- CSCud35416

  Symptom: The Jabber application for iPad failed to register with Cisco Unified Border Element (CUBE). This symptom is also seen when CUBE does not respond to the *out-of-dialog* option pings (TCP), which are sent by the Microsoft Lync server.

  Conditions: This symptom occurs in the following scenarios:

  Default registration with a TCP length longer than 536 bytes, which causes TCP fragment in the Jabber application for iPad.

  When the call flow is as follows: Microsoft Lync Server >> SIP >> Cube.

  The following TCP flow is seen from the packet capture:

  ```
  LYNC     Cube Syn>>>>>> <<<<<<Syn, Ack Ack>>>>>> OPTIONS>> <<<<<<Ack : No SIP 200 OK
  was sent by the CUBE.
  ```
  Workaround: Use the following workaround options:

  - Configure the **ip tcp adjust** *1400* command.
  - Downgrade to Cisco IOS Release 15.2(3)T2.

- CSCud50029

  Symptom: TX drops seen on LSMPI driver **show platform software infrastructure lsmpi driver** command:

  ```
  Reason for TX drops (sticky):     Bad packet len   : 0     Bad buf len      : 0
  Bad ifindex      : 0     No device        : 0     No skbuff        : 0     Device xmit
  fail : 663  <<<<< ......
  ```
  Conditions: Counter increase due to large or bursty control packets.

  Workaround: There is no workaround.

- CSCue14143
- CSCue45934

  Symptoms: This problem is specific to the Catalyst 6000 platform. With IPv4 crypto map, ICMP echo reply is not triggered from the remote end.

  Conditions: This symptom is observed in IPv4 crypto map configuration and Catalyst 6000 platform.

Workaround: There is no workaround.

- CSCue50255

  Symptom: ucode crashes @ ucode crash@REM_REM_MISC_ERR_LEAF_INT_INT_REM_POP_REQ_TO_EMPTY_SCHE

  Conditions: This condition occurs 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:

  1. Before doing a load version from RP0 (initial active), enter the s**how ipv6 route** [**table | inc IPv6**] command:
  2. Note down the number of IPv6 route tables in the system.
  3. Do a load version.
  4. Wait for standby to come up to Standby hot.
  5. Enable the standby console from RP0 (active).

     ```
     asr1000#configure terminal
     asr1000(config)#redundancy
     asr1000(config-red)#main-cpu
     asr1000(config-r-mc)#standby console enable
     ```

  6. Log in to the standby console and enter the **how ipv6 route** [**table | inc IPv6**] command. Then, note down the number of IPv6 route tables in standby. If the number is lesser than the number noted in Step 2. wait for some time and re-verify till it reaches the number noted in Step 2.
  7. Issue ISSU run version from RP0 (active).

- CSCue63742

  Symptom: Tracebacks are seen in a basic call scenario.

  Conditions: CTI call flow is enabled.

  Workaround: Do not configure CTI (allow watch) in ephone-dn.

- CSCue69527

  Symptoms: More than 95 SCCP controlled FXS ports cannot be configured on the Cisco VG350. The debug output for the **debug ccm-manager config-download errors** command 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.

- CSCue80506

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

Conditions: When there is a routing issue such that the Cisco ASR 1000 Series Aggregation Services Router acting as the DMVPN hub can receive spoke registrations but does not have a valid route to the spoke (i.e. the spoke's forwarding interface is Null 0) and the spoke's QoS configuration include a queuing feature, then the QoS policy is not applied and the ESP has to be reloaded to recover from this problem.

Workaround: There is no workaround, but the following actions can get the router operational again:

- Correct the routing issue and reload the ESP.
- Remove the QoS queuing feature and reload the ESP.

- CSCue88077

  Symptom: Router reloads with traceback pointing to voip_rtcp_session.

  Conditions: This issue is seen for SIP-H323 calls at 50 CPS in CUBE (Ent) configuration.

  Workaround: There is no workaround.

- CSCue94694

  Symptom: cpp_cp_svr crash @ cpp_ifm_if_delete_cntx is seen.

  Conditions: This condition occurs while removing PVCs and invalid interfaces.

  Workaround: There is no workaround.

- CSCuf93395

  Symptom: Traceback is observed in HUB on FP reload.

  Conditions: QoS is not applied in hardware when traceback occurs. This occurs when QoS is applied to a spoke's tunnel on the DMVPN hub following the flapping of a spoke's tunnel.

  Workaround: Reload the ESP.

- CSCug34404

  Symptom: RP crash is seen at be_interface_action_remove_old_sadb.

  Conditions: The symptom is observed while unconfiguring the 4K SVTI sessions after an HA test.

  Workaround: There is no workaround.

- CSCug52953

  Symptom: Reload of QFP occurs with one of the following backtraces:

  - Driver Interrupt: DPE5_CPE_CPE_DPE_INT_SET_0_LEAF_INT_INT_S4_WPT_ERROR

  ```
  BackTrace # 0 hal_abort () at
  /scratch/mcpre/BLD-BLD_V153_3_S_XE310_THROTTLE_LATEST_20130428_224613/cpp/dp/hardware/
  cpp/hal/hal_logger.c:81 #1  0x8032998a in tw_fire_timer_events () at
  /scratch/mcpre/BLD-BLD_V153_3_S_XE310_THROTTLE_LATEST_20130428_224613/cpp/dp/infra/log
  ger.h:207 #2  0x8032a4bc in time_process_timer_hb () at
  /scratch/mcpre/BLD-BLD_V153_3_S_XE310_THROTTLE_LATEST_20130428_224613/cpp/dp/infra/tim
  e.c:837 ...
  ```

  Conditions: These type of cores can appear for various conditions. The particular CDETs only addresses when this condition occurs after unconfiguring NAT PAP mode. This includes changing PAP or BPA configuration.

  Workaround: After unconfiguring PAP, it is recommended to reload the box that is more desirable than an uncontrolled reset.

- 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.

- 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.

- CSCug66565

  Symptom: A previous code commit to address the same issue caused a catastrophic issue wherein SPA is going out of service, during the SPA reload and chasiss reload after the RP switchover on 1 RU. This bug improves the fix so that this catastrophe is not seen again. The original issue was exposed during regression testing while doing an ISSU upgrade.

  Conditions: Aforementioned commit should be present in the image and chassis should be ASR 1001. The issue is seen when SPA is reloaded after RP switchover.

  Workaround: The issue is not seen if :

  - Chassis is not ASR1001.
  - Aforementioned fix is not present in the image.

- CSCug69107

  Symptom: Crypto session does not comes up in EZVPN.

  Conditions: This symptom is observed when a Crypto session is being established.

  Workaround: There is no workaround.

- CSCug73700

  Symptom: Failed to do ISSU in CC/SPA upgrade.

  Conditions: This condition is seen when the user does a subpackage ISSU in a system for only "sip*" packages.

  Workaround: There is no workaround.

- CSCug78153

  Symptom: Traffic drops are seen with FTP NAT PAP mode.

  Conditions: This condition occurs with FTP NAT PAP configured on BOX.

  Workaround: There is no workaround.

- CSCug84557

  Symptom: CUBE SBC does not forward mid-call Re-INVITE in a glare condition.

Conditions: This condition occurs in a glare condition, where both legs of a SIP call through the SBC sends in re-INVITE within 100 ms of each call. The SBC is expected to forward the first arriving Re-INVITE to the other leg and then reject the second call with a 491 Request Pending response. Instead, the SBC does not forward either of the Re-INVITE, and gets into a deadlock condition leading to no audio and eventual call tear down.

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.

- CSCug91447

  Symptom: Packets are lost on transmission to an MLP bundle. Lost packets show up in drop statistics as tail drops.

  Conditions: This condition occurs after removal and re-insertion of SPA module, which contains one or more links in the MLP bundle.

  Workaround: After the SPA re-insertion, remove the serial link from the bundle and add it back.

- CSCug95485

  Symptom: UUT is crashing.

  Conditions: This condition occurs after switching from default mode to CGN mode, sending multiple sessions of PPTP.

  Workaround: There is no workaround.

- CSCug97823

  Symptom: On the latest Cisco IOS XE 3.10 throttle build, when the VRF-Lite GM starts registering to the KS, many of these error messages flood the console continuously.

  ```
  %IMGR-6-FIPS_FMFP_N2_ERR_FAIL: SIP0: fman_fp_image:  Cryptographic coprocessor
  non-critical failure: stats multi context read error.
  ```

  Conditions: This condition occurs on ASR 1002-X (KingPin) Chassis acting as VRF-Lite GM with as less as 400 GMs registering to the KS.

  Workaround: There is no workaround. Turning off Crypto feature will stop these messages, which is not an preferred option at this time.

- 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.

- CSCuh06678

Symptom: One local address can be mapped to multiple global addresses.

Conditions: This condition occurs with PAP configured.

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.

- CSCuh11994

  Symptom: pp_svr crash is noticed executing the **show platform hardware cpp active infrastructure punt policer handle 1000 cpp** command.

  Conditions: This condition is noticed without any feature configurations.

  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.

- CSCuh14012

  Symptom: The crypto session remains UP-ACTIVE after tunnels are brought down administratively.

  Conditions: This symptom occurs in tunnels with the same IPsec profile with a shared keyword.

  Workaround: There is no workaround.

- CSCuh23109

  Symptom: ISR4400: as a cube crash at PC = 0x7f2edf875555 Conditions: ISR-4451 Configured as CUBE (SIP-SIP) crashed under traffic.

```
Image:
v153_2_s_xe39_throttle-BLD-BLD_V153_2_S_XE39_THROTTLE_LATEST_20130407_111216-ios 169
Type of traffic Call Flow:
Phone-A--------CUCM--------CUSP-----(CUBE-ISR4451)------CUSP-------CUBE-ISR3900-----CU
CM----PhoneB  The Traffic was running at the a rate of 200 concurrent calls.
========= Exception Tracebacks ==============================================
Exception to IOS: Frame pointer 0x7F2E9EEF5B38, PC = 0x7F2EDF875555 IOS Thread
backtrace:  UNIX-EXT-SIGNAL: Aborted(6), Process = VoIP FPI Process -Traceback=
1#afd249001e68409960c31d5c87971049  c:7F2EDF844000 31555  Fastpath Thread backtrace:
-Traceback= 1#afd249001e68409960c31d5c87971049  c:7F2EDF844000 BE002  Auxiliary Thread
backtrace:             -Traceback= 1#afd249001e68409960c31d5c87971049
pthread:7F2ED6E5F000 A7C9
```

  Workaround: Disable detailed stats:

```
ASR#conf t
ASR(config)#voice service voip
ASR(conf-voi-serv)#media disable-detailed-stats
```

- CSCuh27146

  Symptom: qfp crash

  Conditions: Topology: Landslide A -- > TC -- > ASR1000 -- > asr5000

  Workaround: No More Info:

- CSCuh33069

  Symptom: qfp crash

  Conditions: handoff from gtpv0 to gtpv1

  Workaround: no More Info:

- 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.

- CSCuh42885

  Symptom: Changing modes in CGN and sending traffic results in ucode crash.

  Conditions: Unconfiguring one mode and switching to another mode and sending traffic.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCuh57618

Symptom: The gateway sends the **Subscription-State Terminated** NOTIFY message before receiving an unsubscribe request.

Conditions: This symptom occurs when the router is loaded with the *c2900-universalk9-mz.SPA.153-2.25.M0.1* image.

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

- CSCuh63682

  Symptom: Router crash in autoamtic test. The trigger to the crash is the following show command: **show flow monitor** *name* **cache format csv**.

  Conditions: No delay between configuration phase and show command execution.

  Workaround: Delay of 10 seconds between configuration phase and show command execution. The crash is not seen in manual testing.

- CSCuh74069

  Symptom: Super-package MDR ISSU fails with the following message: MDR:FAILED: Insufficient memory available on harddisk: to support MDR.

  Conditions: Super-package MDR ISSU operation is issued.

  Workaround: Issue sub-package MDR ISSU.

- 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.

- 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
  ```

- 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.

- CSCui06014

  Symptom: Create 2000 GRE IPSEC tunnels (sample config shown below, repeated 2000 times) causes RP crash.

  ```
  interface tunnel10001     bandwidth 1000     ipv6 address 1003:0:0:1::1/64     ipv6
  enable     tunnel source Loopback10001     tunnel dest 1004:0:1:1::1     tunnel mode
  gre ipv6       tunnel protection ipsec profile hub10001
  ```

  Conditions: On ISR4400, it is tested to work fine when scaled up to 1000 sessions. At 1500, we have observed the crash. The in between numbers are not available. On ASR 1K, it is tested to work fine when scaled up to 2500 sessions. At 4000, the crash is observed. The in between numbers are not available.

  Workaround: Bring up the tunnels in staggered manner (booting with the configs can also cause the issue) by shutdown the interface and unshut in batches.

- CSCui09501

  Symptom: RP_Crash seen @__be_crypto_ipsec_key_engine_sa_req.

  Conditions: While unconfiguring the vrfs on spoke-side.

  Workaround: There is no workaround.

- CSCui14994

  Symptom: A router may exhibit GPM errors similar to the following:

  ```
  %INFRA-3-INVALID_GPM_ACCESS_DATA: 67605cec63f8a9dc   f3431ea743899b9a
  50a4d7fe457c725a   d4fb26d18422c310   1d6f875f5802d283    43238:   F0: cpp_cp: QFP:0.0
  Thread:009 TS:00007383841341196593 %INFRA-3-INVALID_GPM_ACCESS_INFO:  820064c0
  0002fd70  00022290  00000011  0002fdb0  00000000  00000011  00000000  805610ea
  000340be  00000000  00000016  00000020  000340aa  00000067  00000032    43237:   F0:
  cpp_cp: QFP:0.0 Thread:009 TS:00007383841340894106 %INFRA-3-INVALID_GPM_ACCESS:
  Invalid GPM Load at 805610ef HAL start 3fc0 HAL end 40bf INFRA start 409c INFRA 40c0
  NET 340aa
  ```

  Conditions: These are the result of incorrect fragmented packet processing internally, specifically as it relates to UDP traffic.

  Workaround: There is no workaround.

- CSCub56842

  Symptoms: The router stops passing IPsec traffic after some time.

  Conditions: This symptom is observed when the <CmdBold>show crypto eli<noCmdBold> 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 SW.

  Workaround: Reload the router before active sessions reach the max value. To verify, do as follows:

  ```
  router# show 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 <<<
  ```

- 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.

- CSCuh36750

  Symptom: ESP crashes.

  Conditions: Subscriber session with QoS over tunnel or shaped VLAN.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- CSCue29351

  Symptom: Caller continuously hears ringback tone while callee is able to hear the caller. Only when the callee presses the Hold and Resume button, two-way audio is established.

  Conditions: Call Flow
  PSTN----(VIC2-4FXO)GWY(29XX)----H323--CM(8.6.2.23047-2)--HTTP-ECC---Phone

  Issue impact cu has workaround, that is, call works when MTP is invoked; but when MTP is invoked, the multicast MOH fails to work. Troubleshooting is performed. This issue is not seen when the call is made directly to the phone without being routed through ECC. Using H323 Slow start or Fast start does not make a difference.

  Workaround: When MTP is enabled on H323 GWY, there is no issue.

- 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:

  Workaround: There is no workaround.

- CSCue40120

  Symptom: Small packet performance for multicast traffic has unexpected dip with 03.07.01S on ESP40

  Conditions: A change made while optimizing performance for ESP100/FP100 and ESP200/FP200 was to use the internal recycle queue for the root of the replication tree instead of the **leaves** recycle queue used for all other nodes. Unknowingly, this resulted in a big performance impact on the ESP40.

  Workaround: Small packet performance can be returned to acceptable levels by disabling MLRE with the **platform multicast lre off** configuration command. The downside of disabling MLRE is that large packet performance are reduced by almost half for large packets.

- CSCue43895

  Symptom: The **show crypto gdoi gm dataplane counters** and **show crypto gdoi gm replay** commands show negative or very large counters.

  Conditions: The **clear crypto sa counters** command is issued after the **clear crypto gdoi dataplane counters** command and **clear crypto gdoi replay counter** command for a GETVPN or GDOI Group Member (GM) running IOS version 15.3(2)S/T or later with the **show crypto gdoi feature long-sa-lifetime** command being available.

  Workaround: Do not issue the **clear crypto gdoi dataplane counters**, **clear crypto gdoi replay counter**, and **clear crypto sa counters** commands simultaneously, and if counters go negative or become very large, execute the **clear crypto gdoi** command to reset the Group Member (GM).

Note GM will remove IPsec SAs and re-register, causing some traffic drop.

- CSCue45131

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

  Conditions: This issue happens when you reboot the router.

  Workaround: Reload ESP.

- 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.

- CSCue62227

  Symptom: SIP PSTN gateway may delay response to BYE message at the end of a T.38 call.

  Conditions: Incoming call to SIP gateway goes out a PRI Call successfully switches no T.38 BYE is received by SIP gateway. 200 OK response is delayed by a few seconds.

  Workaround: There is no workaround.

- CSCue69906

  Symptom: Video calls are failing with improper call legs.

  Conditions: After doing testcase-specific configurations, the basic call is done. while checking the call legs after the call is connected, improper call-legs are seen on CUBE3.

  Workaround: There is no workaround.

- CSCue77317

  Symptom: Incorrect SGT tag for IPSec packets.

  Conditions: Enable CTS for IPSEC.

  Workaround: There is no workaround.

- CSCuf35359

  Symptom: Traceback appears.

  Conditions: Both PBR and WCCP are configured.

  Workaround: Reload.

- 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:

- CSCug32688

  Symptom: DNS query failure occurs occasionally with MPLS deployed.

  Conditions: This symptom occurs under the following conditions:

  - DNS server response 5k
  - Inside MPLS interface, default MTU
  - Repeat dns query for serveral times

  Workaround: Set MPLS MTU to 9216 or change TCP MSS on both client-server side.

- 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.

- 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.

- 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.

- CSCug53833

  Symptom: When attaching or detaching performence monitor to or from interface, memory is leaking.

  ```
  <conf t>  perf mon context perf-mon prof appl     traffic-monitor all
  <conf t>  interface GigabitEthernet0/0/3
  performance monitor context perf-mon
  no performance monitor context perf-mon
  ```

  Conditions: FAll tools avc config.

  Workaround: There is no workaround.

- CSCug59729

  Symptom: An ASR1001 may reload when used as a hub in a scaled DMVPN environment.

  Conditions: This is seen when the traffic rates approaches the limit of the encryption capabilities of the router.

  Workaround: There is no workaround.

- CSCug65706

  Symptom: Attaching performence monitor to OTV interface should be blocked.

  ```
  <conf t>   interface Overlay1
  otv control-group 239.1.1.1
  service-policy type performance-monitor output new-policy ==> this configuration line
  should be blocked.
  ```

  Conditions: FAll tools avc config.

  Workaround: There is no workaround.

- CSCug68282

  Symptom: ASR1000 RP crash after software upgrade.

  ```
  Apr 20 09:53:01.396: %SYS-3-BADBLOCK: Bad block pointer 3AFDF4B0 -Traceback=
  1#b3d7956825375323829953c9aa18e3e0  :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#b3d7956825375323829953c9aa18e3e0  :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#b3d7956825375323829953c9aa18e3e0
  c:86FA000 368B4 c:86FA000 368B4 c:86FA000 384C8 :10000000 32FD91C :10000000 1F227BC
  :10000000 1F1C1B0 :10000000 1F3F750   Fastpath Thread backtrace:  -Traceback=
  1#b3d7956825375323829953c9aa18e3e0  c:86FA000 D9F08 c:86FA000 D9EE8 iosd_unix:887E000
  1580C pthread:7DB2000 5A4C   Auxiliary Thread backtrace:  -Traceback=
  1#b3d7956825375323829953c9aa18e3e0  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).

- 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.

- CSCug73476

  Symptom: Customer is running a CME environment with Cisco 2901 Series Router. Once or twice every week during high call volume, the soft key such as Transfer and End Call stops responding.

  Conditions: Once phone sends **EndCall** soft key (0x26) to CUCME, the CUCME does not send **CallState** (0x111), **CloseReceiveChannel** (0x106), and **StopMediaTransmission** (0x8B) to phone. Therefore, the call is not terminated.

  Workaround: After pressing **TRANSFER** soft key, do not abort the transfer by pressing the **Abort** soft key.

- CSCug81259

  Symptom: During configuring performance monitor, and when the registration to CFT fails, the router crashes.

  Conditions: FAll tools AVC configuration.

  Workaround: There is no workaround.

- 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.

- CSCug86082

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

  Conditions: When all the following conditions meet, this bug will show up:

  – The call is setup as NAT call.

  – Media is received before offer or answer is completed.

  – The call is modified to hairpin with other calls both on two sides.

Workaround: The following workaround's are possible:

- Disable NAT.
- Do not send media untill offer or asnwer is completed.

- 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.

- 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.

- CSCug97705

  Symptom: Configured PPTP Timeout is not taking effect on Translations for PPTP ALG.

  Conditions: Sending Traffic for PPTP-ALG.

  Workaround: There is no workaround.

- CSCuh06849

  Symptom: Fragmented PPTP ALG traffic may not be processed as expected.

  Conditions: Fragmented PPTP ALG traffic may be dropped, with NAT PAT configuration.

  Workaround: Turn off PPTP ALG if not required.

- 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.

- CSCuh12779

  Symptom: The ASR1k does not reply to IPv6 ping packets sent to its LISP IPv6 EID address, when these are received over a LISP IPv4 RLOC space.

  Conditions: This condition only applies to ICMPv6 echo reply packets, that are generated on the RP, and received over an IPv4 RLOC core. Pinging other IPv6 hosts in the LISP site works fine. The reply is generated on the RP, but dropped before it leaves the box.

  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).

- CSCuh18253

  Symptom: GTPv2 message with invalid IMSI is not dropped.

  Conditions: Invalid IMSI is used.

  Workaround: There is no workaround.

- CSCuh32165

  Symptom: CVLA memory is not released. Check FNF_AOR CVLA for memory usage. show platform hardware qfp active infrastructure cvla client handles <snip>

  ```
  Entity name: FNF_AOR Handle: 2344906752 Number of allocations: 176 Memory allocated:
  14144 <snip> show platform hardware qfp active  feature fnf datapath aor <snip>
  Extracted Field objects        Alloc                    1200               0
  Free                         100 <snip>
  ```

  Conditions: AVC with IPv6 protocol.

  Workaround: There is no workaround.

- CSCuh48261

  Symptom: Tunnel entry are deleted together.

  Conditions: Primary PDP context and secondary PDP context. tear down ind is 0 in delete PDP context request.

  Workaround: There is no workaround.

- CSCuh48747

  Symptom: Multiple NAT entries are created.

  Conditions: UUT is configured with PAT with route-map.

  Workaround: There is no workaround.

- CSCuh59216

  Symptom: Dedicated bearer is failed to be setup.

  Conditions: Dedicated bearer.

  Workaround: There is no workaround.

- CSCuh71310

  Symptom: Modify bearer response is dropped.

  Conditions: Control plane teid in modify bearer request is changed from teid in create session request.

  Workaround: There is no workaround.

- CSCuh73986

  Symptom: DNS response get dropped with no-payload being configured and NAT FW.

  Conditions: Configure NAT FW (DNS inspect), send DNS query from inside, server then reply to the response.

  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.

- CSCuh98929

  Symptom: IFNF supports a single L3 byte counter for a connection. There are no separate counters for connection between the client and server. This fix adds client and server counters.

  Conditions: The following commands are supported: **flow record test** and **collect counter bytes long end**

  With this fix, two additional counters can be collected: flow record test and collect counter bytes long collect connection client counter bytes network long collect connection client counter bytes server long end

  Workaround: There is no workaround.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.1S

This section describes the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.1S. It contains the following topics:

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.1S

This section documents the unexpected behavior that may be seen in Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.1S.

- 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.

- CSCts95896

  Symptom: The router does not pass traffic on EVC interfaces.

  Conditions: Occurs when you issue the default interface command to remove a configuration containing approximately 400 EVC interfaces and immediately enter a new EVC configuration.

Workaround: Wait for the router to clear pending objects before adding a new configuration.

- CSCtx72973

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

  Conditions: Seen on HA setup.

  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).

- CSCty24937

  Symptom: TCAM exhaustion and FP crash with IDFW scale > 300 class-maps on 2ru or rp1/rp10 box.

  Conditions: None.

  Workaround: There is no workaround.

- CSCua28807

  Symptom: NHRP redirect message is getting dropped at FlexServer's Tunnel Interface which results in direct spoke-spoke tunnel failure.

  Conditions: Whenever there is a data traffic initiated from spoke1's host network to remote spoke's host network.

  Workaround: There is no workaround. However the data traffic will be successful through hub, even though the direct spoke-spoke channel is not ps.

- 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.

- CSCub29339

  Symptom: FP10 crashes with v6GRE configured and IPv4 multicast traffic.

  Conditions: FP10 crashes with v6GRE configured and when IPv4 multicast traffic is passed.

  Workaround: There is no workaround.

- CSCuc84675

  Symptom: ASR1k crash.

  Conditions: Billing enabled.

  Workaround: There is no workaround.

- CSCuc97950

  Symptom: Performance drop with MPLSoGRE.

  Conditions: Performance drop with MPLSoGRE.

  Workaround: There is no workaround.

- CSCud24378

  Symptom: Traffic rate verification fails.

  Conditions: After QoS configuration changes.

  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.

- CSCud71871

  Symptom: High CPU on ASR hub on scale setup.

  Conditions: Scale set up with 4 K DMVPN session.

  Workaround: There is no workaround.

- CSCud75278

  Symptom: ATM event trace is holding too many memory (about 16 MB) even if ATM feature is not enabled.

  Conditions: Router is active.

  Workaround: Change the event trace size manually to a small value:

  ```
  infra-asr1001-4(config)#monitor event-trace platform atm size ?  <1-1000000> Number
  of entries in trace.
  ```

- CSCud78578

  Symptom: RP crashes after FP switchover.

  Conditions: FP(FP80) reload with qos configs and traffic flowing in the background.

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**.

- CSCue12146

  Symptom: APN active PDP counter may show incorrect values in cases where PDP(s) fails to be properly activated. If APN default gateway is configured with an address outside the GGSN session IP Address pool subnet, a GTP session cannot be initiated. APN active PDP counter will be incremented even though no sessions are established as seen in the following:

  ```
  Router#sh gtp apn 1   apn_index   : 1           apn_name = 3gp.cisco.com GGSN Addr
  : 89.0.0.1        Primary DNS : 0.0.0.0         DHCP Addr   : 12.0.0.1        DHCP
  Lease: 1800 Tunnel MTU  : 1460 IPv6 prefix len  : 64 Number of active PDPs in this
  APN : 10     <<<<<<<<<<<<< INVALID COUNTER  Default GW     Prefix Length Name
  MAC Address     PDP Count 12.0.0.1        16                          aaaa.bbbb.cccc
  0 Router#sh gtp pdp all Router#sh sss session %No active Subscriber Sessions Router#
  ```

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCue14586

  Symptom: After reload, system may not be able to bring up all ipsec tunnels at high scale (1k) group members.

  Conditions: ASR1K with GETVPN, 1k group members.

  Workaround: Issue **clear crypto gdoi** to force re-registration and rebuild of tunnels.

- CSCue34749

  Symptom: SIP Crashes on RP switchover.

  Conditions: Issue is seen in scale setup.

  Workaround: Reload SIP.

- CSCue35100

  Symptom: Performance drop is seen in IPv6 multicast related feature.

  Conditions: In RP2/ESP40.

  Workaround: There is no workaround.

- CSCue48456

  Symptom: Call is disconnected through CUBE.

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

  Workaround: There is no workaround.

- CSCue50255

  Symptom: ucode crashes at `REM_REM_MISC_ERR_LEAF_INT_INT_REM_POP_REQ_TO_EMPTY_SCHE`

  Conditions: On flapping multilink interfaces

  Workaround: There is no workaround.

- CSCue50484

  Symptom: Crypto Tunnel Socket remains open after shutting the tunnel interface.

  Conditions: Dual-DmVPN with ike-profile on the tunnel interface.

  Workaround: There is no workaround.

- CSCue53562

  Symptom: Crypto Tunnel Socket remains open after shutting the tunnel interface.

  Conditions: Dual-DmVPN with ike-profile on the tunnel interface.

  Workaround: There is no workaround.

- CSCue65190

  Symptom: FP crash.

  Conditions: Sending traffic at high rate and performing bpa configuration change.

  Workaround: Send traffic at low rate.

- CSCue69527

  Symptom: More than 95 SCCP controlled FXS ports cannot be configured on 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.

- CSCue80506

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

  Conditions: DMVPN, NHRP, QOS.

  Workaround: There is no workaround.

- CSCue88077

  Symptom: Router reloads with traceback pointing to voip_rtcp_session.

  Conditions: This issue is seen for SIP-H323 calls at 50 CPS in CUBE(Ent) configuration.

  Workaround: There is no workaround.

- CSCue91054

  Symptom: ESP Crashes when sending IPv6 fragmented traffic through dmvpn hub(mgre tunnel).

  Conditions: This happens when sending big IPv6 packets (need to do IPv6 fragmenation after adding tunnel header) traffic through dmvpn hub(mgre tunnel). Large amout of IPv6 fragment traffic (example: 5G on ESP20) which exceeds reassembly performance number (less than 2G).

  Workaround: Change mtu to avoid IPv6 fragmentation.

- CSCuf65537

  Symptom: Crash with CAC with Contact center call flow.

  Conditions: Crash is observed with CAC configurations and 40 cps call rate:
  `UNIX-EXT-SIGNAL: Segmentation fault(11), Process = RSCCAC CALL DENIAL SCAN -Traceback= 1#0ac7b601f45270393178c559213c70ba :400000 344C0D0 :400000 699DCD1 :400000 344C43B :400000 344C386 :400000 344C6B0 :400000 699D248.`

Workaround: There is no workaround.

- CSCuf66382

  Symptom: 90% CPU utilization by crypto IKMP process on primary KS server with scale setup.

  Conditions: The topology is 2KS (primary is Overlord and secondary is ASR 1004) with 10 groups and 100 GMs register per group for a total of 1000 GMs.

  Workaround: There is no workaround.

- CSCuf74266

  Symptom: ASR-CUBE: Crash observed with DSMP.

  Conditions: Load scenario issue is observed.

  Workaround: There is no workaround.

- CSCuf82128

  Symptom: ASR-CUBE: Crash observed with DSMP.

  Conditions: Load scenario issue is observed.

  Workaround: There is no workaround.

- CSCuf85233

  Symptom: ESP core was found after sh debug execution was done immediately after reload.

  Conditions: ESP process is down.

  Workaround: Delay of approximately 60 seconds is required without any interruption.

- CSCuf96663

  Symptom: Memory leaks seen with Smap-Dmap scale scenario, 4K sessions.

  Conditions: Leaks seen after stress testing : rekey , dpd, clear commands.

  Workaround: There is no workaround.

- CSCuf96673

  Symptom: Memory leaks seen with Smap-Dmap scale scenario, 4K sessions.

  Conditions: Leaks seen after stress testing : rekey , dpd, clear commands.

  Workaround: There is no workaround.

- CSCug04450

  Symptom: PfR fails to control traffic classes with subnet mask greater than the length of the prefix.

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

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

- CSCug19588

  Symptom: IKEv2 TPS performance degradation over time.

  Conditions: This occurs in the lab under extreme test conditions with traffic running during session bring-up.

  Workaround: Reduce traffic and or reduce session bring-up rate.

- CSCug21859

  Symptom: ASR1k crashes on receiving broken packet with NBAR configured on the NAT interface.

Conditions: ASR1k DNS packet coming (broken at L4 header), NBAR configured (**match protocol dns**), NAT with vasi interfaces.

Workaround: There is no workaround.

- CSCug27362

  Symptom: Packet drop occurs.

  Conditions: Packet drop occurs when IPSEC VTI IPv6 tunnels are configured on an ESP100/FP100 . The following message appears: `%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: Remove the IPSec configuration between the tunnels.

- CSCug28249

  Symptom: On enabling NAT inside on a ASR router with 10 Gigiabit Ethernet interfaces, the ESP crashes. The packet in question is a DNS packet. The time between enabling NAT inside and from when the ESP crashes may vary depending on traffic conditions.

  Conditions: NAT must be enabled inside.

  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.

- CSCug39612

  Symptom: BDI interface stops forwarding traffic as seen in the output of **show interface bdi <number>**

  Conditions: After creating 20 to 50 BDIs (approximately), BDI interface stops forwarding traffic.

  Workaround: Reload the router. However, the issue will be seen once in every 24 to 48 hours.

- CSCug42528

  Symptom: ESP stops forwarding traffic with following error messages:

  ```
  Mar 26 17:11:38.504 UTC: %IOSXE-2-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:089
  TS:00006032009661609351 %HAL_PKTMEM-2-OUT_OF_RESOURCES:  Mar 26 17:12:38.536 UTC:
  %IOSXE-2-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:019 TS:00006032069706815681
  %HAL_PKTMEM-2-OUT_OF_RESOURCES:  Mar 26 17:13:38.907 UTC: %IOSXE-2-PLATFORM: F0:
  cpp_cp: QFP:0.0 Thread:107 TS:00006032130075669937 %HAL_PKTMEM-2-OUT_OF_RESOURCES:
  Mar 26 17:14:38.987 UTC: %IOSXE-2-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:103
  TS:00006032190158892360 %HAL_PKTMEM-2-OUT_OF_RESOURCES:  Mar 26 17:15:43.939 UTC:
  %IOSXE-2-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:123 TS:00006032250425485709
  %HAL_PKTMEM-2-OUT_OF_RESOURCES:   Service was recovered after the router reload,
  however monitoring shows a stable trend in PKTMEM utilization:  stj-core-r01#sh
  platform hardware qfp active bqs 0 packet-buffer utilization Packet buffer memory
  utilization details:   Total:     128.00 MB   Used :     87.65 MB   Free :   41322.50
  KB   Utilization:  68 %          <--------- rising constantly   Threshold Values:
  Out of Memory (OOM)    :     127.96 MB, Status: False     Vital (> 98%)         :
  125.44 MB, Status: False     Out of Resource (OOR)  :     108.80 MB, Status: False
  ```

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCug45740

  Symptom: Latency on high priority flows coming on onboard Gigabit Ethernet interfaces when the system is oversubscribed.

  Conditions: ISR4400 platform.

  Workaround: There is no workaround.

- CSCug45840

  Symptom: Cisco ASR1000 routers do not detect spurious memory accesses.

  Conditions: This symptom occurs when a bug is present that causes a read from the lowest 16 KB of memory.

  Workaround: There is no workaround.

- CSCug48145

  Symptom: ASR DTMF interworking failed after re-invite with block configured.

  Conditions: DTMF with different preferences configured results in this issue.

  Workaround: There is no workaround.

- CSCug50397

  Symptom: PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT IOS thread disabled interrupt for 33 msec -Traceback= 1#37814e8bffa827ad4b7cd9006e6e91fa :400000 89DB43 :400000 3EFB074 :400000 3EFB84A :400000 27D65B3 :400000 27B9697 :400000 731F4F9 :400000 4E17047 :400000 2579B62 :400000 256B14B :400000 2568FDE

  Conditions: There are no known conditions.

  Workaround: Reload the router to accept any CLI command.

- CSCug52953

  Symptom: Reload of QFP occurs with 1 of the following backtraces.

  - Driver Interrupt: `DPE5_CPE_CPE_DPE_INT_SET_0_LEAF_INT_INT_S4_WPT_ERROR`
  - BackTrace #0 hal_abort () at `/scratch/mcpre/BLD-BLD_V153_3_S_XE310_THROTTLE_LATEST_20130428_224613/cpp/dp/hardware/cpp/hal/hal_logger.c:81 #1 0x8032998a in tw_fire_timer_events () at /scratch/mcpre/BLD-BLD_V153_3_S_XE310_THROTTLE_LATEST_20130428_224613/cpp/dp/infra/logger.h:207 #2 0x8032a4bc in time_process_timer_hb () at /scratch/mcpre/BLD-BLD_V153_3_S_XE310_THROTTLE_LATEST_20130428_224613/cpp/dp/infra/time.c:837 ...`

  Conditions: These type of cores can appear under various conditions. The particular CDETs only address when this condition occurs after unconfiguring NAT PAP mode. This includes changing PAP or BPA configuration.

  Workaround: After unconfiguring PAP, it is recommended to reload the box which is more desirable than an uncontrolled reset.

- CSCug53833

  Symptom: Minor memory leakage at QuantumFlow Processor (QFP), caused by MMA.

  Conditions: When configuring and un-configuring performance monitor (MMA).

  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 sent CurrentLevel Varbind, but should send csbQOSAlertCurrentValue Varbind.

  Conditions: When CUBE SP generates voice quality alerts.

  Workaround: The code fix is included in 15.2(4)S4. Manually clean the alarm at CUOM after root cause is rectified, if earlier CUBE version is used.

- CSCug65706

  Symptom: Configuring MMA on an Overlay Transport Virtualization (OTV) interface may cause a CPP Ucode crash.

  Workaround: Do not configure MMA on an OTV interface.

- CSCug70875

  Symptom: Active FP/ESP crashes causing switchover to standby.

  Conditions: AVC/CFT configurations being tested on the box.

  Workaround: There is no workaround.

- CSCug73700

  Symptom: Failed to do ISSU in CC/SPA upgrade. MDR compatibility verification fails stating target version is the same as the running version, as shown below:

  ```
  Starting mdr compatibility verification Non-upgrade MDR ISSU operation from [X] to
  [X] is not supported for CC in slot [n] As SIPn does not support MDR none of the SPA's
  within in may be upgraded using MDR FAILED: MDR compatibility failed
  ```

  Conditions: ISSU with Subpackage MDR only. Not applicable to superpackage MDR.

  Workaround: Specify elc images at the same time as sipbase and sipspa packages.

- CSCug76838

  Symptom: RP crashed multiple times due to SBC main process.

  Conditions: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SBC main process. Observed in 15.2(1)S version.

  Workaround: There is no workaround.

- CSCug77212

  Symptom: ASR1K CUBE RP may crash with Segmentation fault(11), Process = CCSIP_SPI_CONTROL when sip headers are manipulated using a sip profile for 200 response messages for KPML notify.

  Conditions: Crash seems to be happening due to SIP profiles configs being wrongly applied to Notify response (this profile was meant for 200 OK Invite response).

  Workaround: Do not configure sip profiles to manipulate the headers for 200 responses.

- CSCug78153

  Symptom: Traffic drops seen with FTP NAT PAP mode.

  Conditions: with FTP NAT PAP configured on BOX.

Workaround: There is no workaround.

- CSCug79517

  Symptom: Router crashed due to software exception.

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCug82494

  Symptom: BGP session with neighbor flaps.

  Conditions: Occurs when BGP and WCCP configured at the same time.

  Workaround: Configure **deny tcp any any** at the end of redirect ACL list.

- CSCug84557

  Symptom: CUBE SBC does not forward mid-call Re-INVITE in a glare condition.

  Conditions: In a glare condition where both legs of a SIP call through the SBC and sends in Re-INVITE within 100ms of each other. Instead of forwarding the first arriving Re-INVITE to the other leg and then rejecting the other with a 491 Request Pending response, SBC does not forward either of the Re-INVITE and gets into a deadlock condition leading to no audio and eventually call tear down.

  Workaround: There is no workaround.

- 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.

- CSCug91447

  Symptom: Taildrop in UUT.

  Conditions: Perform SPA OIR in UUT configured with one multilink bundle.

  Workaround: There is no workaround.

- CSCug92878

  Symptom: The ESP may crash when activating and deactivating NBAR in a fast long cycle.

  The ESP log (cpp_cp_F0.log) contains the following error message:

  ```
  add feature to instance - feature 'STILE' already exists in instance 'GLOBAL_CFT'
  ```

  Conditions: The crash is seen on version v153_2_s_xe39_throttle, when an implicit/explicit fast automatic cycle of NBAR is activated/deactivated.
  The chance of an ESP crash occuring in a common case scenario is very rare as it depends on timing. Therefore, different platforms may exhibit different scenarios.

  Workaround: There is no workaround.

- CSCug96781

  Symptom: QFP crash.

Conditions: TC is used.

Workaround: There is no workaround.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.1S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.1S.

- CSCtg13667

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

  Conditions: Issue is observed on ASR1k running 15.0(01)S code.

  Workaround: There is no workaround.

- CSCts83413

  Symptom: While configuring Classic Netflow to export records to a user specified VRF, the user configuration can get out of sync or be invalid such that the QFP Processor does not have the same VRF information as is present in the IOS configuration. Thus, the configuration is out of sync and Netflow export does not function.
  This symptom may also be observed while configuring Flexible Netflow.

  Conditions: Multiple cycles of VRF configuration as well as multiple cycles of Netflow export destinations have taken place. The IOS configuration was to export to a particular VRF (for example: VRF "BLUE"), while the QFP processor had a configuration to export to the default VRF.

  Workaround: To restore Netflow export fucntionality, unconfigure the Netflow export destination and reconfigure it.

- CSCty59423

  Symptom: Memory leak at IPIP channels.

  Conditions: The conditions are unknown. The following is a sample error message that appears:
  `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`

  Workaround: There is no workaround.

- CSCub79487

  Symptom: Traffic flow is not fine with Fragementation.

  Conditions: None.

  Workaround: There is no workaround.

- CSCuc11849

  Symptom: Packets of smaller lengths (less than 100 Bytes) may be dropped occasionally when a shaper is configured.

  Conditions: This issue occurs when a shaper is configured on CSR1000V and traffic consisting of smaller packet lengths (less than 100 Bytes) are sent below the configured shape rate.

  Workaround: There is no workaround.

- CSCuc31339

  Symptom: An error message similar to the following appears: `%ASR1000_INFRA-3-EOBC_SOCK: R0/0: linux_iosd-image: Socket event for EO0, fd 16, failed to send 1472 Bytes; Resource temporarily unavailable.`

  Conditions: Large number of feature configurations exist.

  Workaround: There is no workaround.

- CSCuc59979

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

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

  Workaround: There is no workaround.

- CSCud19536

  Symptom: A short AVC2.0 downtime is experienced after modifying the AVC2.0 configuration.

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

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

- CSCud29930

  Symptom: A Cisco ASR1002-X with built-in SPA may record runts on its Gigabit Ethernet interfaces when using a SFP-GE-T (copper). This issue is not seen with an SFP-GE-S (fiber).

  Conditions: This issue occurs for any frame that requires Ethernet padding to be added to make it 64 Bytes.

  Workaround: There is no workaround.

- CSCud34173

  Symptom: Many statistics shown by the Entreprise Service Gateway crypto engine are zero and these are not relevant to crypto engine in ISR4400. This is due to the reason that there is no separate Hardware crypto engine on the ISR4400 platform for encrypt/decrypt operations. The Data plane processor executes the encrypt/decrypt functions using software in addition to other feature software execution. The Control plane has hardware support for general crypto operations (such as getting Random number and ModExp operations).

  Conditions: IPSEC is in use.

  Workaround: There is no workaround to see the aggregate statistics for the encrypt/decrypt operations performed by software in Data Plane processor.

  The following counters in the output of **show platform hardware crypto-device statistics** display these statistics. The remaining statistics in the output of this command (which are shown as 0) must be ignored:

```
PROCESSED(P)    :          27374510, PROCESSED(B)    :                0
ENCRYPTED(P)    :          13686332, ENCRYPTED(B)    :          1204397216
DECRYPTED(P)    :          13688119, DECRYPTED(B)    :          930792092  GEN.
PURPOSE(P)  :                    0 , GEN. PURPOSE(B)  :                  0
```

- CSCud56611

  Symptom: Traffic flow fails with VRF aware IPSec while using crypto maps.

  Conditions: VRF configuration on the **iskamp** or **ikev2** profile is changed.

  Workaround: Remove and re-apply crypto map on the interface.

- CSCud64870

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

  Conditions: The crash happens when there are five CDPs for the hub router to fetch the 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 one CDP instead of multiple CDPs avoids the timing condition which leads to the crash.

- CSCud67112

  Symptom: The IPv6 traffic with **nbar** protocol may not be classified correctly.

  Conditions: When **nbar** protocol is configured with IPv6.

  Workaround: There is no workaround.

- CSCud67653

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

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

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

- CSCud70629

  Symptom: Incremental memory leaks are seen at IPSec background proc.

  Conditions: This symptom is observed with **clear nhrp cache**.

  Workaround: There is no workaround.

- CSCud81272

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

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

  1. Config the NAT.

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

  3. Check messages.

  Workaround: There is no workaround.

- CSCud90061

  Symptom: When executing a route processor (RP) switchover, the console CLI may display an error message beginning with `CPPOSLIB-3-ERROR_NOTIFY`. This symptom does not affect functionality and does not require any action to be taken.

  Conditions: Can occur when executing a route processor (RP) switchover and does not impact any functionality.

  Workaround: There is no workaround.

- CSCud99438

  Symptom: With VRF-lite config and **permit ip any any**, incoming traffic is dropped.

  Conditions: Different VRFs and **permit ip any any**.

  Workaround: There is no workaround.

- CSCue04941

  Symptom: When CSR1000v is being used as a VPN gateway and BFD session, the number of stable BFD sessions is lower than expected.

  Conditions: When CSR1000v is being used as a VPN gateway and BFD session, the number of stable BFD sessions is lower than expected.

  Workaround: There is no workaround.

- 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 **no ccm-manager config** to stop the config download from CUCM.

- CSCue22731

  Symptom: WCCP service cannot work.

  Conditions: Two services are configured in same interface, and then one service is deleted while the other is inactive.

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

- CSCue22764

  Symptom: **ip wccp check acl outbound** does not work on Ultra/Overlord.

  Conditions: Ultra/Overlord platform.

  Workaround: There is no workaround.

- CSCue25575

  Symptom: The crash is observed for SDP pass through or call forward or anti-trombone cases.

  Conditions: The crash is observed for a basic call involving SDP pass through call forward anti-trombone cases.

  Workaround: There is no workaround.

- CSCue34694

  Symptom: 2921 Router crashed after receiving 486 Busy.

  Conditions: Observed when handling 486 Busy response.

  Workaround: There is no workaround.

- CSCue35533

  Symptom: Ping fails with security applied and IKE disabled.

  Conditions: This symptom is observed when the Cisco IOS Release 15.3(1.15)T image is loaded.

  Workaround: There is no workaround.

- CSCue36387

  Symptom: When IPv6 crypto is applied, the inbound interface counters associated with the crypto configuration are not updated correctly. There is no problem with the functionality but the counters are incorrect.

  Conditions: Problem seen with interface input counters when using IPv6 crypto.

  Workaround: There is no workaround.

- CSCue37523

  Symptom: When IOS is a IPSEC QM (Quick Mode) responder for ipsec, and if it receives QM1 packet from Call Manager with missing ID payload, the packet is processed, but QM2 packet is not sent to the Call Manager. It works fine when IOS is the initiator of QM.

  Conditions: IOS Responder to QM from call manager does not send ID payload in transport mode in QM1.

  Workaround:

  1. Initiate traffic from IOS router so that IOS is a QM initiator.

  2. Change config of racoon client on call manager to send ID payload in QM1 as initiator (support_proxy on).

- CSCue40138

  Symptom: sip parse error in case of retransmission.

  Conditions: tcp retransmission with segments.

  Workaround: There is no workaround.

- CSCue41031

  Symptom: Exta IPsec flow is shown in the **show crypto session** output.

  Conditions: This symptom is observed with the Cisco ASR 1000 RP1 FlexVPN Client.

  Workaround: There is no workaround.

- CSCue45952

  Symptom: **Retransmitting phase 2 QM_IDLE** seen in debugs and Phase2 information is resent after successful IPSec tunnel establishment, causing tunnel teardown.

  Conditions: Seen only if the following conditions are met:

  - Certificate authentication is used
  - There is no traffic on the tunnel

  This DDTS is exposed by the commit of DDTS CSCua36739.

  Workaround: Generate traffic, for example via IP SLA. All the branches where the fix for CSCua36739 is published, need this fix as well.

- CSCue46222

  Symptom: When CSR1000v is used as a VPN gateway and has zone based firewall with AVC configured, the NDR value for 72 Byte packets is lower than expected.

  Conditions: When CSR1000v is used as a VPN gateway and has zone based firewall with AVC configured, the NDR value for 72 Byte packets is lower than expected.

  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 IP Security (IPSec) termination and aggregation.

  Workaround: There is no workaround.

- CSCue47463

  Symptom: Certain ASR1K platform-specific CLI commands are accepted on the console, but a **not supported** message is displayed.

  Conditions: This issue is seen with on ISR4400 routers.

  Workaround: There is no workaround.

- CSCue47940

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

  Conditions: After a reboot.

  Workaround: There is no workaround.

- CSCue48143

  Symptom: BQS feature is not supported on ISR routers, therefor BQS show commands do not provide any output. Example: **ISR4451#show platform hardware qfp active bqs 0 cif ISR44515#show platform hardware qfp active bqs 0 fif ISR4451#show platform hardware qfp active bqs 0 gif ISR4451#**

  Conditions: None.

  Workaround: Ignore BQS commands, as BQS feature is not supported on ISR4451.

- CSCue48243

  Symptom: Undefined event is displayed instead of an event related to registration.

  Conditions: Seen when **show monitor event gdoi registration all** CLI is executed.

  Workaround: There is no workaround.

- CSCue51792

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

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

  Workaround: Use one of the following:

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

- CSCue52065

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

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

  Workaround: There is no workaround.

- CSCue53207

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

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

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

- “connection delay application sum” is dependent on:

  connection delay response to-server sum

  connection delay network to-server sum

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

  connection delay response to-server min

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

  connection delay response to-server max

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

  connection delay response to-server sum

  connection delay network to-server sum

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

  connection delay response to-server min

  connection delay network to-server sum

  connection server response sum

  connection delay response to-server sum

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

  connection delay response to-server max

  connection delay network to-server sum

  connection server response sum

  connection delay response to-server sum

  connection delay network to-server max

- CSCue59759

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

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

  Workaround: There is no workaround.

- CSCue61481

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

  Conditions: Hard OIR

  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.

- CSCue68258

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

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

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

  show platform software object-manager FP active statistics

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

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

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

- CSCue69960

  Symptom: Traceback and Queuing error for interface AppNav-Compress interface.

  Conditions: Upon disabling the service context, saving config and reload.

  Workaround: Upon enabling service-context, traceback is no longer seen.

- CSCue71931

  Symptom: Traceback is seen as soon the router reloads.

  Conditions: This is an intermittent issue seen when the router reloads and at the same time WCM sends a sync message to apply the configuration. We have 2 channels trying to apply config at the same time.

  Workaround: Reload the router again.

- 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**

- CSCue77265

  Symptom: Increment memory leaks are seen at IPSec background proc.

  Conditions: This symptom occurs when clear cry session is issued multiple times when bringing up the tunnel.

  Workaround: There is no workaround.

- 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: Use the same platform for all PfR Border Routers.

- CSCue83147

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

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

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

  Workaround: There is no workaround.

- CSCue85415

  Symptom: For CSCue40506, KS uses 1 acl with 4 ace, and GM applies the same gdoi cm on 500 interfaces. This config creates four flows (which is expected), but around 2000 (and sometime 4000) dummy aces.

  Conditions: getvpn lisp scaling.

  Workaround: Use the same platform for all 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.

- CSCue85737

  Symptom: ASR with PKI certificate may crash when issuing **<CmdBold>show crypto pki certificate<noCmdBold>** command.

Conditions: This symptom is observed when the **<CmdBold>show crypto pki certificate<noCmdBold>** command is issued on ASR with PKI certificate.

Workaround: There is no workaround.

- CSCue87308

  Symptom: All incoming lisp packets are dropped with cause IpLispHashLkupFailed in overlord(ISR4400) platform.

```
shmcp-ovld-1#shdrop
------------------------------------------------------------------
------- Global Drop Stats                      Packets
Octets
------------------------------------------------------------------
------- IpLispHashLkupFailed                    2007
0
```

  Conditions: Basic lisp traffic.

  Workaround: There is no workaround.

- CSCue87883

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

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

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

- CSCue88591

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

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

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

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

- CSCue89006

  Symptom: SIP ALG creates PAT translation before portlist.

  Conditions: This is a SIP ALG cooperation for consistency with NAT modification on defect.

  CSCuc85157 for PAT. This resolves a problem since v. XE37.

  Workaround: There is no workaround

- CSCue89491

  Symptom: GM tries to re-register after the rekey mechanism change.

  Conditions: When the user changes rekey transport type and waits for the schedule to take place.

  Workaround: After changing rekey transport type, issue **crypto gdoi ks rekey** to send the rekey instead of waiting for schedule rekey.

- CSCue89658

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

  Conditions: When a process encounters a defect, it causes the generation of a core file. The system is supposed to wait to finish generating a core file. But, if a second critical process encounters a defect concurrent to the first process, then the system starts the shutdown procedure before the first process is finished with generating a core file. As part of the shutdown procedure, the manager of the hardware watchdog is shutdown. This causes a kernel panic in about 120 seconds. If the first process does not finish generating the core file, then a kernel panic occurs. This leads to generating a kernel core file, and terminates generation of the core file of the first process before it can complete.

  Workaround: There is no workaround.

- CSCue90034

  Symptom: Router cannot boot up.

  Conditions: Seen on certain configurations.

  Workaround: There is no workaround.

- CSCue92716

  Symptom: Variable length exceeding 256 characters may cause issues.

  Conditions: Traffic with HTTP extracted fields with length exceeding 1 Byte.

  Workaround: Use traffic with HTTP fields with length less than 1 Byte.

- CSCue93355

  Symptom: GM failed to register with KS.

  Conditions: SGT tagging enabled.

  Workaround: There is no workaround.

- CSCue94610

  Symptom: 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: The following command may clear up the DSPs:

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

- CSCue96079

  Symptom: There is out of memory traceback on ASR1K router.

  Conditions: Too many sessions are created which is over scale limitation.

  Workaround: Clear a few sessions.

- CSCue97118

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

Conditions: Very large From header in incoming SIP invite.

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

- CSCue97338

  Symptom: Update PDP context request is dropped.

  Conditions: TEID is 0, IMSI is existing.

  Workaround: There is no workaround.

- CSCue97986

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

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

  Workaround: There is no workaround.

- CSCuf00166

  Symptom: With GM Local ACL (deny), traffic must be sent clearly but is dropped instead.

  Conditions: GM Local ACL (deny) is configured on GM and running image with CSCuc87266 fixed.

  Workaround: There is no workaround.

- CSCuf01088

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

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

  Workaround: There is no workaround.

- CSCuf02990

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

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

  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**.

- CSCuf04906

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

  Conditions: Crashes under load conditions.

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

- 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.

- CSCuf15260

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

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

  Workaround: Do not change DTMF type mid-call.

- 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.

- CSCuf21611

  Symptom: TDM Voice call is terminated due to voice-port shutdown when T1/E1 module on other NIM slot is reloaded (OIR).

  Conditions: OIR of T1/E1 module in any NIM slot shuts down the voice ports (if any) on all other T1/E1 NIM slots.

  Workaround: There is no workaround.

- CSCuf24592

  Symptom: 1. Certain counter values will appear to wrap around for condition 1 under the section "Aggregate traffic distribution statistics". 2. Certain counter values will appear to decrement instead of incrementing for condition 2 under the section "Aggregate traffic distribution statistics". The following fields are affected: `Packet and byte counts ---------- Redirected Bytes Redirected Packets Received Bytes Received Packets Occurrences ----------`

  `Initial Redirects Initial Redirects Accepted Initial Redirect -> Passthrough Redirect -> Passthrough`

  Conditions: 1. When counter values exceed 4294967296. 2. When one of the following clear commands are run and the value exceeds 4294967292: **clear service-insertion statistics, clear service-insertion statistics service-node, clear service-insertion statistics service-node-group**.

  The symptom is observed when viewing the output from either of the two show commands **show service-insertion statistics service-node** or **show service-insertion statistics service-node-group**.

  Workaround: Avoid issuing the **clear service-insertion statistics service-node-group** and **clear service-insertion statistics service-node** commands. We can monitor the stats for the counter values up to 2^32 and wraparound thereafter. This limit the counter values to 2^32 instead of 2^64.

- CSCuf25027

  Symptom: Substantial drop in performance. High latency and packets drop.

Conditions: Router is configured with full AVC config (NBAR,ART,QoS) and Ipsec. This issue is seen with high traffic (more than 500 Mbps). Packet drops can be verified by issuing this command: **show platform hardware qfp active statistics drop clear**

The following is an example of the outpout of this command:

```
Global Drop Stats                          Packets                  Octets
-------------------------------------------------------------------------------
IpsecOutput                    3250          3242721 Ipv4NoAdj
797              1056357 PuntErr                                  1
276   <B>Workaround:</B> Disable AVC from the interface.
```

Workaround: Disable AVC from the interface.

- CSCuf25232

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

  Conditions: Not known. See also CSCtz08251 and CSCua92010.

  Workaround: There is no workaround.

- CSCuf25318

  Symptom: ESP crashes when executing **show platform hardware qfp active feature fnf client application name MMA**

  Conditions: The performance monitor has five or more traffic monitors, or if there are more than eight monitors that bind to the application. Example: performance monitor context my-visibility profile application-experience traffic-monitor application-response-time traffic-monitor conversation-traffic-stats traffic-monitor url traffic-monitor media traffic-monitor application-traffic-stats interface GigabitEthernet0/0/3 performance monitor context my-visibility.

  Workaround: Execute object and instance separately instead of the default like: show platform hardware qfp active feature fnf client application name MMA object show platform hardware qfp active feature fnf client application name MMA inst. The default is to show both object and instances and this is crashing if there are more than eight instances. Therefore, do not use the following in that case: show platform hardware qfp active feature fnf client application name MMA

- 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. The system does not crash with FTP stateful traffic.

- CSCuf29962

  Symptom: Aggressive alert is seen when no alert is set.

  Conditions: ZBFW is on and alert is seen after disabling the parameter-map type inspect global and clearing drops.

  Workaround: There is no workaround.

- CSCuf34496

  Symptom: Router crashing when T1/E1 module is reloaded (OIR) with active TDM calls on another T1/E1 module on same router.

  Conditions: OIR of a module with or without any configurations, along with another module with active TDM calls is leading to a crash.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCuf46942

  Symptom: When the router receiving the SYN is reloaded, traffic is not optimized after the router has come up. This occurs with ACG scenario and asymmetric scenario.

  Conditions: Immediately after router reload.

  Workaround: There is no workaround.

- CSCuf47717

  Symptom: A major alarm is listed indicating that the node is not reachable even though the cluster is up and operational.

  Conditions: This happens on switchover from Active to Standby.

  Workaround: The alarm can be cleared with disable and enable of service context.

- CSCuf49959

  Symptom: Router crashes when tunnel interface is flapped.

  Conditions: When sessions are there, do shut/no shut multiple times.

  Workaround: There is no workaround.

- CSCuf51801

  Symptom: The CLI command **show crypto session xxx** results in memory leaks.

  Conditions: Execution of **show crypto** CLI command appears to cause 168 Byte memory leak for each of the following commands: **- show crypto session brief - show crypto session local <IP> brief - show crypto session local <Mac> brief - show crypto session remote <Mac> brief - show crypto session remote <Mac> brief - show crypto session username <any> brief - show crypto tech-support peer <IP> - show crypto tech-support**.

  Workaround: There is no workaround.

- CSCuf51881

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

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

  Workaround: There is no workaround.

- CSCuf56693

  Symptom: 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.

- CSCuf57226

  Symptom: Scheduler is not handling gratuitous arp packets properly before dataplane comes up.

  Conditions: Scheduler is not handling gratuitous arp packets properly before dataplane comes up.

  Workaround: There is no workaround.

- 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.

- CSCuf65404

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

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

  Workaround: There is no workaround.

- CSCuf68548

  Symptom: ccpp_cp_svr and fman_fp cores during mdr.

  Conditions: While doing spa/SIP OIR during mdr.

  Workaround: There is no workaround.

- CSCuf78259

  Symptom: cWAAS optimized traffic cannot pass ZBF zone-pair.

  Conditions: WCCP outbound is used, and WAAS optimization enabled.

  Workaround: Configure WCCP inbound rather than outbound, or disable ZBF.

- 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.

- CSCuf82550

  Symptom: The fragment issue is seen in lisp getvpn, and flapping ipsec sessions. After 2 to 3 hours, the console reports a series memory fragment error and traceback. After several hours, cef will be disabled. IOS Router displays malloc failure error message.

  Conditions: lisp getvpn flapping IPSec session.

  Workaround: There is no workaround.

- CSCuf85449

  Symptom: Crash at be_ewag_gtp_path_pdp_remove_one during session churns.

Conditions: 48K EoGRE sessions of mix GTP (18K) PMIP (18K) and SIP (12K). During session churning, GTP crash is observed.

Workaround: There is no workaround.

- CSCuf90643

  Symptom: WRED state not completely reset between packets causing drop policy to work incorrectly.

  Conditions: If a class has WRED fair queue and another class with fair queue, then average depth calculation is done on wrong queue causing functionality issue.

  Workaround: Do not use class with fair queue when there is another class with WRED and fair queue.

- 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.

- CSCuf98264

  Symptom: An incorrect error is printed when trying to update the maximum back-off time.

  Conditions: The symptom occurs only when CPU regulation is enabled (it is disabled by default) and the user wants to update the maximum back-off time.

  Workaround: Use the default back-off time.

- 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.

- CSCug04287

  Symptom: Tunnels may fail to come up without warning.

  Conditions: When there is a limit on tunnels or on unlicensed routers.

  Workaround: There is no workaround.

- 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.

- CSCug04947

  Symptom: Ucode may crash with high FTP ALG traffic NAT PAT configraution.

  Conditions: Ucode may crash with high FTP ALG traffic NAT PAT configuration.

  Workaround: Turn off all ALGs with **no ip nat service**. Use static or dynamic NAT configuration.

- CSCug09187

  Symptom: A router crash can be observed with console logging a message: `"UNIX-EXT-SIGNAL: Segmentation fault(11), Process = EWAG GTP PDP 1" when trying to bring up GTP sessions.`

  Conditions: A misconfigured subscriber profile without "cisco-msisdn" configured in AAA for a GTP subscriber will cause the crash.

  Workaround: **cisco-msisdn** is mandatory IE for iWAG GTP. It must be present in AAA profile.

- CSCug11093

  Symptom: The following message is logged: 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.

  Workaround: There is no workaround.

- CSCug11220

  Symptom: GETVPN ipv6 packets get dropped.

  Conditions: None.

  Workaround: There is no workaround.

- CSCug12997

  Symptom: Router crash with the following message:

  ```
  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: During normal operation.

  Workaround: There is no workaround.

- CSCug14039

  Symptom: Router crashes when all three subslots are 8-port E1 and all are configured with PRI voice.

  Conditions: When router boots up, the voice port creation will cause the router to crash.

  Workaround: There is no workaround.

- CSCug14060

  Symptom: Booting a Cisco ISR 4450 router with three NIMs (fully populated) with a 3.9.0 IOS XE release image for the first time may see a reset of the router. The problem is not seen on subsequent boot up. The reset may be seen with the following syslog message.

  ```
  %PMAN-0-PROCFAILCRIT:pvp.sh: A critical process cmcc has failed (rc 134)
  %PMAN-5-EXITACTION:pvp.sh: Process manager is exiting: critical process fault, cmcc,
  cc_0_0, rc=134 %PMAN-5-EXITACTION: Process manager is exiting: reload fru action
  requested
  ```

  Conditions: Cisco ISR 4450 router needs to have 3 NIMs plugged in to the system, and system is booting IOS XE 3.9.0 release for the first time.

  Workaround: Reset the system one more time. This issue is not seen again after a reset.

- 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.

- CSCug20100

  Symptom: Traffic drop as PaWalkErr.

  Conditions: NAT FTP IPSEC on ovld.

  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.

- 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 256 Bytes.

  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.

- 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 example:
  ip nat inside source list 1 pool pool1 overload

- CSCug36251

  Symptom: GETVPN KS downloaded TEK / IPsec policy handling on the GM which is now "Centralized" across both ASR and ISR to support Suite-B policy (i.e. a "permit A B" will install its SA's as as A => B for both INBOUND and OUTBOUND). Previously, the ISR platform installed GETVPN TEK / IPsec policy as "Site-to-Site" where a "permit A B" will install its SA's as A => B for OUTBOUND and B => A for INBOUND.

  Conditions: None.

  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.

- CSCug44944

  Symptom: vg350-universalk9-mz.SSA image fails to build.

  Conditions: Building image fails.

  Workaround: There is no workaround.

- CSCug45964

  Symptom: PAP reference count (viewed via 'sh pl h q a f nat data pap') is too high. The PAP reference count should match the number of sessions referencing that local address. This will cause NAT memory footprint to be higher than expected because the PAP entries are not properly freed in this case.

  Conditions: This issue can only happen when PAP is configured ('ip nat setting pap') and certain types of ALG traffic is run.

  Workaround: Issuing a **clear ip nat trans** periodically will remove the stranded PAP entries and prevent the NAT memory footprint from buidling up.

- CSCug49130

  Symptom: KP crashes with FTP traffic.

  Conditions: When NAT is configured in CGN mode with PAP.

  Workaround: There is no workaround.

- CSCug49843

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

  Conditions: OUT_OCT_DETECT_SEQ_OVEFLOW counter increase.

  Workaround: There is no workaround.

- CSCug51847

  Symptom: RP crash is observed when the following command is issued:

  <CmdBold>show gtp pdp imsi <CmdArg> IMSI <noCmdArg><noCmdBold>

  Conditions: This crash happens only when the above command is issued to show the detail of a gtp pdp, which is in **dns look up pending** state.

  Workaround: There is no workaround.

- CSCug57503

  Symptom: ESP crash.

  Conditions: Executing **show platform hardware qfp active feature packet-trace configuration**.

  Workaround: Do not execute unsupported command.

- CSCug61097

  Symptom: In some traffic conditions, running AVC configuration on the ASR1002-X platform may lead to a crash.

  Conditions: Under heavy load and with specific traffic pattern, usually found at ISP network, running AVC configuration on ASR1002-X may lead to a crash.

  Workaround: There is no workaround.

- CSCug63419

  Symptom: Call coming from CUCM on a SIP Trunk to ISR4400 platform and goes out on a PRI Trunk on the same ISR4400 platform.

Conditions: Call is coming on a SIP dialpeer and goes out on a POTS dialpeer and router crashes.

Workaround: There is no workaround.

- CSCug65541

  Symptom: Traceback observed at **service_controller_delete_sc_node** on performing RP switchover.

  Conditions: On performing RP switchover and when the ASR is registered with the CM.

  Workaround: There is no workaround.

- CSCug76754

  Symptom: ISR4451 Crashed under traffic.

  Conditions: ISR4451, crashed when used as CUBE under extended traffic.

```
Software Version:  Cisco IOS Software, IOS-XE Software
(X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version 15.3(20130501:122311)
[v153_2_s_xe39_throttle-BLD-BLD_V153_2_S_XE39_THROTTLE_LATEST_20130501_111211-ios
170]  CallFlow:
Phone-A-------------CUCM10.0-----------------CUSP------------------(ISR4451-CUBE)
-------------------------CUSP---------------ISR-3900-CUBE----------------CUSM10.0
----------------PhoneB  Type of traffic:  SIP-SIP  (Basic and Supplementary Services)
Traffic Rate:  200 Concurrent calls.  TRACEBACK 1#1b67e6e760d4ea492a73b51cd18661d7
:400000 74BD589 :400000 78F5760 :400000 790432B :400000 78EBDC9 :400000 78E6B06
:400000 7915DE2
```

  Workaround: There is no workaround.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.0S

This section describes the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.0S. It contains the following topics:

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.0S

- CSCtw74124

  Symptom: For a slot housing ASR1000-SIP40, or on ASR1002-X, the output of the **show platform hardware slot <slot#> plim buffer settings detail** command will show the value of Max always as 0 against Fill Status Curr/Max, 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.

- CSCuc59324

  Symptom: Errors while executing the **request platform software package clean** command.

Conditions: After executing subpackage ISSU upgrade procedure, the **request platform software package clean command** is giving errors.

Workaround: There is no workaround.

- CSCud19536

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

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

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

- CSCud30442

  Symptoms: On a Cisco ASR1002 router, the **show platform hardware crypto-device context packet count** does not display correctly.

  Conditions: Cisco ASR1002 router.

  Workaround: There is no workaround.

- CSCud47058

  Symptom: Committed Memory value 96% exceeds warning level 95% on 4RU ISSU SIP upgrade.

  Conditions: This symptom is observed when performing a SIP ISSU upgrade in a 4RU.

  Workaround: This is just a warning message. There is no impact on the functionality or the traffic.

- CSCud56245

  Symptom: Error is seen during post router clean up %CWAN_HA-4-IFEVENT_BULKSYNCFAIL: receive failed ifevent: 10 error: 3.

  Conditions: Error message seen in the Release 15.3(02)S image on mcp_dev.

  Workaround: There is no workaround.

- CSCud59647

  Symptoms: On a ASR1002 router, the configure wrong static routes point to ipsec tunnel, and cpp crashes under high rate traffic.

  Conditions: Cisco ASR1002 router.

  Workaround: no workaround.

- CSCud67112

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

  Conditions: May occur with IPv6 HTTP traffic.

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

- CSCud90061

  Symptom: When executing a route processor (RP) switchover, the console CLI may display an error message beginning with “CPPOSLIB-3-ERROR_NOTIFY”. The symptom does not affect functionality and does not require any action to be taken.

  Conditions: Can occur when executing a route processor (RP) switchover.

  Workaround: There is no workaround.

- CSCud91780

  Symptom: RP crashes pointing to REDUNDANCY FSM.

Conditions: This symptom is observed when an active RP crashes or is reloaded.

Workaround: There is no workaround.

- CSCue08522

  Symptom: Traffic loss when over 95% DS3 line rate in 2CHT3-CE-ATM SPA.

  Conditions: None

  Workaround: There is no workaround.

- CSCue26791

  Symptom: On scaled configs with mcast/oif, tracebacks are seen.

  Conditions: On bootup with scaled configs `PLATFORM_INTR_OVER_LIMITS` are seen.

  Workaround: Boot with empty configs and then apply the scaled configs.

- CSCue29276

  Symptom: Embedded Services Processor (ESP) board may be out of service due to run out of process memory.

  Conditions: This symptom is observed on a Cisco ASR1000 series router when functions as an IP Security (IPSec) termination and aggregation router, and when dual-stack (over IPv6 transport) Dynamic Multipoint VPN (DMVPN) is deployed with high scaling of spokes, and with Netflow, NAT, URPF features enabled. And when Route Processor (RP) switch-over happens.

  Workaround: there is no workaround.

- CSCue53207

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

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

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

  - “connection delay application sum” is dependent on:

    connection delay response to-server sum

    connection delay network to-server sum

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

    connection delay response to-server min

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

    connection delay response to-server max

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

    connection delay response to-server sum

connection delay network to-server sum

connection server response sum

– "connection delay response client-to-server min" is dependent on:

connection delay response to-server min

connection delay network to-server sum

connection server response sum

connection delay response to-server sum

connection delay network to-server min.

– "connection delay response client-to-server max" is dependent on:

connection delay response to-server max

connection delay network to-server sum

connection server response sum

connection delay response to-server sum

connection delay network to-server max

- CSCue63092

  Symptom: The Application ID field shows up as 0.

  Conditions: ICA traffic is sent through a ASR functioning as a single ANC in an ACG.

  Workaround: There is no workaround.

- CSCue69960

  Symptom: Traceback and Queuing error for interface AppNav-Compress interface.

  Conditions: Upon disabling the service context, saving config and reload.

  Workaround: Upon enabling service-context, traceback is no longer seen.

- CSCue77228

  Symptom: The show service-insertion statistics connection summary command displays large pass-through flows (greater than two million). This issue only affects the summary output. The non-summary output is not affected.

  Conditions: Multiple AppNav Controllers in an AppNav Controller Group is configured.

  Workaround: Use non-summary output to count flows.

- CSCue71931

  Symptom: Traceback is seen as soon the router reloads.

  Conditions: This is an intermittent issue seen when the router reloads and at the same time WCM sends a sync message to apply the configuration. We have 2 channels trying to apply config at the same time.

  Workaround: Reload the router again.

- CSCue71667

  Symptom: ISR-WAAS service deployment fails when using EZConfig and a network/broadcast address as the service IP.

  Conditions: When using EZConfig for enabling ISR-WAAS service, if a network or broadcast address is used as the service IP, EZConfig does not complain and goes ahead and tries to install, activate service and register the same with WCM, which fails.

Workaround: Use a valid IP address for service IP, other than loopback address, network address, and broadcast address.

- CSCue80399

  Symptom: Fails to remove SN_OR_WCM class and ACL config after 'service waas disable' process.

  Conditions: 1. Activate and ensure ISR-WAAS is up and running with cms status online 2. Reload router after "wr mem" is performed on the router and ISR-WAAS. 3. Ensure that the ISR-WAAS boots up with the required configs and cms status online. 4. With/without De-Register ISR-WAAS from CM. 5. Perform a 'service waas disable' and ensure all the configurations performed through 'service waas enable' is removed.

  Workaround: Remove the SN_OR_WCM class and ACL manually.

- CSCuf24592

  Symptom: 1. Certain counter values will appear to wrap around for condition 1 under the section "Aggregate traffic distribution statistics". 2. Certain counter values will appear to decrement instead of incrementing for condition 2 under the section "Aggregate traffic distribution statistics". The following fields are affected: `Packet and byte counts ---------- Redirected Bytes Redirected Packets Received Bytes Received Packets Occurrences ----------- Initial Redirects Initial Redirects Accepted Initial Redirect -> Passthrough Redirect -> Passthrough`

  Conditions: 1. When counter values exceed 4294967296. 2. When one of the following clear commands are run and the value exceeds 4294967292: **clear service-insertion statistics**, **clear service-insertion statistics service-node**, **clear service-insertion statistics service-node-group**. The symptom is observed when viewing the output from either of the two show commands **show service-insertion statistics service-node** or **show service-insertion statistics service-node-group**.

  Workaround: Avoid issuing the **clear service-insertion statistics service-node-group** and **clear service-insertion statistics service-node** commands. We can monitor the stats for the counter values up to 2^32 and wraparound thereafter. This limit the counter values to 2^32 instead of 2^64.

- CSCue49361

  Symptoms: Jumbo packet drop due to re-assemble timeout.

  Condition: On a Cisco ASR1002 router with NAT64 and Firewall configured, the traffic is GRE tunnel over ipsec in and GRE tunnel over ipsec out. On the egress tunnel, you have to configure "ip virtual-reassembly", otherwise you will observe a jumbo packet drop due to the re-assemble timeout.

  Workaround: Configure "ip virtual-reassembly" on GRE tunnel over ipsec.

- CSCue51515

  Symptoms: On a Cisco ASR1002 router with NAT64 scenario, send udp port 64 stateless unidirectional traffic firewall shows it is sip pkt. And sh policy-map type inspect zone-pair displays NATed ipv4 address as source address instead of ipv6 source address.

  Conditions: None.

  Workaround: There is no workaround.

- CSCue59629

  Symptom: GM re-registers two times after issuing "clear crypto gdoi ks members" on the KS.

  Conditions: KS has multiple IPSec SAs configured on the GDOI group. GM is an ASR.

  Workaround: There is no workaround.

- CSCue59759

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

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

Workaround: No known workaround.

- CSCue61643

  Symptom: When the encapsulation on pvc is aal5mux.

  Conditions: Ping fails when encapsulation on pvc is aal5mux.

  Workaround: Configure a different encapsulation aal2snap and make it default.

- CSCue67984

  Symptom: Pending objects are seen.

  Conditions: This symptom is observed on an SSO with ATM PVP local switch scaling configuration.

  Workaround: There is no workaround.

- CSCue71282

  Symptom: ISR G2 only supports 1,000,000 cache entries per monitor and thus ISR G3 will support only 1,000,000 entries as well. Future releases of the software will enforce this restriction so configurations that exceed 1,000,000 with this release will not work for subsequent releases.

  Conditions: The number of entries in a flow monitor can be configured using the **flow monitor <name> cache entries <NUMBER of ENTRIES>** command.

  Workaround: It is recommended not to configure more than 1,000,000 cache entries per monitor on the ISR G3 platform, and this will be enforced in future software releases.

- CSCue81059

  Symptom: After the aggressive aging trigger goes off, the number of half open sessions is not consistent for a given set of configurations.

  Conditions: This symptom is observed when ZBFW aggressive aging is configured with inspect action.

  Workaround: There is workaround.

- CSCue88209

  Symptom: Bay based cmcc environmental monitoring works but it does not come up in the **show env** command.

  Condition: None.

  Workaround: There is no workaround.

- 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.

- CSCuf09249

  Symptom: ESP40 is observed to reload.

  Conditions: ESP40 is observed to reload with 100 flexvpn sessions with one FW and qos.

Workaround: There is no workaround.

- CSCuf56693

  Symptom: Router may experience a “free ‘garbage pointer’” crash.

  Conditions: May occur when all of the following are true:

  – The border router is configured with performance routing (PfR).
  – The master controller (MC) router is using NBAR to monitor/control traffic.
  – The “ip nbar custom zzzz tcp range 50000 51000” command is executed one or more times.

  Workaround: Shut down the MC before configuring an NBAR custom protocol.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.0S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.9.0S.

- 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.

- CSCsu57181

  Symptom: When the retransmission number is changed, the next rekey does not reflect this change.

  Conditions: Change the number of retransmissions from 2 to 5, and the number stays at 2; and when changing the retransmissions from 2 to 1, the number of retransmissions stays at 2. This happen for both unicast and multicast rekey.

  Workaround: clear crypto gdoi and start over again.

- CSCsz65576

  Symptom: One or more linecards may fail to boot in an ASR1000 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 symptom is observed with certain combinations of RP2 and ESP10.

  Workaround: There is no workaround.

- CSCtc18691

  Symptom: DRAM Error Correction (ECC) is not properly enabled for memory modules installed on certain ASR1k-CC boards.

  Conditions: For these DIMMs, ECC will not be enabled. The system will not be able to detect or correct any single bit errors which may occur during normal operation.The effect of these uncorrected bit errors could lead to unpredictable system behavior.

  Workaround: The card or 2RU system must have the ROMMON upgraded to either version XNC, XND1, or 15.3(1r)S or later. Upon subsequent restart the system will run with the new ROMMON and ECC will function as expected. For full ROMMON upgrade instructions see:

http://www.cisco.com/en/US/products/ps9343/prod_maintenance_guides_list.html. As a temporary workaround until the ROMMON upgrade can be performed, reset the card in question, this will clear the bit error and normal operation will resume, although ECC will still be disabled.

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCti62247

  Symptoms: If an IPv4 or IPv6 packet is sent to a null interface, a Cisco ASR 1000 series router will not respond with an ICMP or ICMPv6 packet.

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

  Workaround: There is no workaround.

- 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.

- CSCtq81245

  Symptom: SPA-4XCT3/DS0 spa reloads after doing fp reload.

  Conditions: 1. Issue is seen on single fp system. 2. Issue is seen when serial interface are configured on the spa. 3. SPA-4XCT3/DS0 spa is installed in SIP40 only

  Workaround: There is no workaround.

- CSCtr96024

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

  Conditions: 1. The Performance Monitor feature is being used on ASR platform. 2. A flow record of type performance-monitor, which contains more than the maximum allowed fields has been configured. 3. The user is referencing the above flow record in a Performance Monitor policy which

has been attached to a desired interface. The maximum number of fields allowed in a flow record = 30 "timestamp sys-uptime first" field "timestamp sys-uptime last" field. If absent, the timestamp fields are automatically added to the record. However, the total number of fields should still be less than or equal to 32.

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

- CSCts08224

  Symptom: Expected ACL/sessions not found for most of the protocols.

  Conditions: The symptom is observed with expected ACL/sessions.

  Workaround: There is no workaround.

- CSCts52120

  Symptom: Tracebacks are seen for PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT.

  Conditions: This symptom is observed with RPSO.

  Workaround: There is no workaround.

- 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.

- CSCtu54300

  Symptom: Tracebacks are seen when configuring the key server.

  Conditions: This symptom occurs when configuring the key server.

  Workaround: There is no workaround.

- CSCtv93326

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

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

  Workaround: There is no workaround.

- CSCtw72739

  Symptom: The "retry-after" time in a 503 message is not used by the gateway (UAC) and retries seem fixed at 180 seconds.

  Conditions: This symptom is observed when trying to register.

  Workaround: There is no workaround.

- CSCtw74598

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

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

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

- CSCtw76527

  Symptom: The crypto session stays in UP-NO-IKE state.

  Conditions: This symptom occurs when using EzVPN.

  Workaround: There is no workaround.

- CSCtx06895

  Symptom: Command "parameter type urlfpolicy" is not available in "policy-map type inspect urlfilter" configuration mode. This makes it impossible to configure IOS URLF in 15.2(3)T. Unable to call the "trend" keyword in the class-map under the policy-map.

  Conditions: IOS 15.2(3)T and 15.2(1)T2(6) both show the same symptom.

  Workaround: Downgrade to 15.2(2)T1.

- CSCtx1579

  Symptom: An MTP on a Cisco ASR router sends an "ORC ACK" message through CRC for the channel ID that is just received but does not reply to the ORC for the next channel.

  Conditions: The symptom is observed when there is a very short time lapse between the ORC and CRC, say 1 msec.

  Workaround: There is no workaround.

- CSCtx59316

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

  Conditions: This symptom is observed with 3.5.2S and similar release and by current design.

- CSCtx84766

  Symptom: No MOH resource is allocated.

  Conditions: Phone1 calls Phone2 over SIP trunk,Phone2 parks the call (MTP required is checked on SIPT).

  Workaround: There is no workaround.

- CSCtx92716

  Symptom: Cisco IOSd crashes.

  Conditions: This symptom occurs when you remove and add service policies on unsupported interfaces.

  Workaround: There is no workaround.

- CSCty01105

  Symptom: DO-EO Flow Around sip to sip with VCC call fails and causes "CCSIP_SPI_CONTROL" memory leaks.Note: With No transcoder involved in CUBE.

  Conditions: CUBE configured with early offer forced and flow around globally under voice service VoIP and VCC, basic call fails with no transcoder enabled in the CUBE.

  Workaround: Configure Transcoder in CUBE.

- CSCty05282

  Symptom: Last reload reason in "show version" output is seen as LocalSoft after some reloads.

  Conditions: The conditions under which these symptoms are observed is unknown.

  Workaround: There is no workaround.

- CSCty35726

  Symptom: The following is displayed on 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.

- CSCty57856

  Symptom: The Standby router crashes for an SRTP call on Active.

  Conditions: This symptom occurs intermittently. This issue is seen due to a transient scenario, where unstable data from Active is checkpointed on Standby.

  Workaround: There is no workaround.

- CSCty94210

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

  Conditions: None.

  Workaround: There is no workaround.

- CSCtz31720

  Symptom: We get some failed debugs when we try to configure snmp-server CLI.

  Conditions: This symptom is observed when you try to configure snmp-server CLI.

  Workaround: There is no workaround.

- CSCtz49911

  Symptom: Certain attributes received from RADIUS might not be displayed as unsupported by IKEv2; printing messages similar to: *Apr 23 06:50:59.952: IKEv2:unsupported attr type 477 *Apr 23 06:50:59.952: IKEv2:unsupported attr type 476.

  Conditions: Flexvpn on 15.2.2S software, but not exclusive to it.

  Workaround: None should be needed. Attributes should be processed correctly.

- CSCtz50013

  Symptom: Memory leak Seen with HA Configs under load Conditions.

  Conditions: HA under Load Conditions.

  Workaround: There is no workaround.

- CSCtz59258

  Symptom: DSP not released when the IP call leg is abnormally disconnected by SIP SPI. This is not reproducible consistently. It is more of timing issue.

  Conditions: SIP SPI abnormally disconnects the call with out sending 200 OK.

  Workaround: Switch over to the secondary to recover DSP resources.

- CSCtz69527

  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 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.

- CSCtz77702

  Symptom: URI based routing is not working when tel-uri is present in 302 contact header.

  Conditions: Configure call route URL.

  Workaround: There is no workaround.

- CSCtz81129

  Symptom: During OCSP revocation check the trustpoint source interface loopback address is also used as the destination address.

  Conditions: During OCSP revocation check the source interface loopback address is also used as the destination address.

  Workaround: Use the physical interface as the trustpoint source interface.

- CSCtz97197

  Symptom: SIP SPAs go in the out of service state in a scaled subinterface configuration (more than 2000 subinterfaces on a single Gigabit Ethernet port).

  Conditions: This symptom occurs while performing ISSU between the iso1-rp2 and iso2-rp2 Cisco IOS XE Release 3.6S throttle image. After ISSU runversion, the SIP SPAs go in the out of service state. This issue is seen in a heavily scaled configuration. This issue is observed when there are 2000 to 3000 subinterfaces on a single SPA and the following limits are exceeded: Overall Dual stack VRFs per box : 2800 Dual stack limit on interface: 1000.

  Workaround: This issue is not seen in the following scenario: 1. Before doing a load version from RP0 (initial active), issue the following command: asr1000# show ipv6 route table | inc IPv6 2. Note down the number of IPv6 route tables in the system. 3. Do a load version. 4. Wait for standby to come up to Standby hot. 5. Enable the standby console from RP0 (active). asr1000#configure terminal Enter configuration commands, one per line. End with CNTL/Z. asr1000(config)# asr1000(config)#redundancy asr1000(config-red)#main-cpu asr1000(config-r-mc)#standby console enable. 6. Log in to the standby console and issue the following command: asr1000-stby#

show ipv6 route table | inc IPv6 Then, note down the number of IPv6 route tables in standby. If the number is less than the number noted at step 2, wait for some time and reverify till it reaches the number noted in step 2. 7. Issue ISSU runversion from RP0 (active).

- CSCua04668

  Symptom: 3945 voice gateway crashes when the config file is download from CUCM. this is 112 FXS bundle.

  Conditions: Once 96 ports have registered and when we try to register the 97 port on, the gateway will download the config from CUCM the router will crash

  Workaround: One workaround is that we do a "no ccm manager config" this will stop the config download form CUCM, we would then have to do a manual config of the rest of the ports an other is to move to H323 as a protocol instead of MGCP

- CSCua06897

  Symptom: Ikev1 session are not coming up on the spoke after sh/no sh on Hub tunnel interface.

  Conditions: sh/no sh on Hub tunnel interface.

  Workaround: There is no workaround.

- CSCua10477

  Symptom: The ASR1002-X Series Aggregation Services Router with large numbers of MLPPP bundles may experience a crash.

  Conditions: When the ASR1002-X Series Aggregation Services 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.

  Workaround: Keep the number of single-link MLPPP bundles under 4,000, and the total number of multi-member MLPPP bundles under 2,000.

- CSCua12998

  Symptom: Call not going between SCCP and SIP phones.

  Conditions: After configuring "no outbound-proxy" under the "voice register global", SCCP endpoints to SIP endpoints call is successful. After some time (approx. 10 minutes or more), the functionality reverts back to "outbound-proxy system", and the same call fails. The configuration still shows "no outbound-proxy" in the running-configuration.

  Workaround: There is no workaround.

- CSCua14749

  Symptom: Carried-id (source/target) CLI is not taken into effect when configured under dial-peer.

  Conditions: Call-route url configured along with voice source-group CLI.

  Workaround: There is no workaround.

- CSCua16122

  Symptom: %PKI-4-CRLINSERTFAIL: Trustpoint "..." failed to verify CRL signature (error 1815:E_NAME_ENCODING : invalid encoded format for name).

  Conditions: "chain-validation continue" is configured on a local trustpoint that is part of the certificate chain from the root CA to the peer.

  Workaround: Configure either "chain-validation stop" or "revocation-check crl none" on all trustpoints in the chain.

- CSCua27722

Symptom: Netflow TimeStamp may show time drift compared to NTP time. This effect has been judged to be equal to about 50 seconds of lost time per day.

Conditions: Flexible or Traditional Netflow running on either an ESP40 based Forwarding Processor or on an ASR1001 platform.

Workaround: There is no workaround but when the time skew exceeds 10 minutes it should self correct.

- CSCua33788

  Symptom: The router does not pass multicast traffic consistently; only some traffic passes.

  Conditions: Occurs when you configure 255 EVCs spanning across different slots on the router.

  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.

- CSCua39375

  Symptom: Cube Crash with SIP config.

  Conditions: Call flow with forking with update, ie. 183 w/ SDP followed by 180 w/o SDP with a different To body (forked call). A resulting reinvite from CUCM causes CUBE to crash as it is applied to the forked call with no SDP causing the crash. voice class sip-profiles in configuration.

  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.

- CSCua44407

  Symptom: Trace back is seen when user part is greater than 32 characters in incoming 302 response contact header.

  Conditions: CUBE in 302 consume mode. userpart in 302 contact header is greater than 32 characters.

  Workaround: There is no workaround.

- CSCua51898

  Symptom: TGW Failed to send BYE message after 200 OK.

  Conditions: TGW Failed to send BYE message after 200 OK with 15.2(03.16)M0.1.

  Workaround: There is no workaround.

- 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.

- CSCua68736

  Symptom: Source files cannot be referenced in the new project.

  Conditions: New project requirement.

  Workaround: There is no workaround.

- CSCua69578

  Symptom: Cleartext send out from flexVPN VAI interface during session flap.

  Conditions: Session delete and create.

  Workaround: There is no workaround.

- CSCua70065

  Symptom: 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.

- 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.

- CSCua78782

  Symptom: Authentication of EzVPN fails.

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

  Workaround: There is no workaround.

- CSCua90697

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

  Conditions: configurate delay as learning type.

  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.

- CSCua94334

Symptom: Hung calls seen in **show call active voice brief** are as follows: `1502 : 26 36329310ms.1 -1 pid:1 Answer XXXYYY4835 connected dur 00:00:00 tx:0/0 rx:0/0 IP 0.0.0.0:0 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8 pre-ietf TextRelay: off media inactive detected:n media contrl rcvd:n/a timestamp:n/a long duration call detected:n long duration call duration:n/a timestamp:n/a.`

Conditions: This symptom is observed when an inbound H225 call setup request to a CME gateway results in a hung call if a release complete is received while still in alerting state. This issue occurs only when the shared line is configured on the phone and the shared line is not registered.

Workaround: Remove the shared line or register the shared line.

- CSCub04205

  Symptom: Incorrect phone screen display, when an incoming call is forwarded. Specifically, with the following config- `alias 1 666 to 85004001 cfw 85004002 timeout 5` calling from external PSTN phone number ex:0612345678 To 4597, which is translated to 666, first rings the phone 85004001 and when it is ringing, screen phone display is OK. When the call is cfw'd to the second phone (85004002), the screen phone display : `Forward 612345678 For 04929 (850... By 04929 (666) is incorrect.` The number 04929 is corresponding to the external phone number mask in CUCM of an other IP phone. The external phone number mask displayed is the field "name" or "description" of the FIRST ephone recorded in the SRST router (see "call-manager-fallback ephone-dn" attached file), whatever the redirect phone number used the mask is ALWAYS the one of the first ephone recorded.

  Conditions: 1. SRST 2. alias command, under call-manager-fallback.

  Workaround: There is no workaround.

- CSCub07288

  Symptom: Path Confirmation fails between 2 SIP phones in a blind transfer scenario over SIP trunk.

  Conditions: This symptom is observed when no supplementary-service SIP refer is configured.

  Workaround: Configure supplementary-service SIP refer.

- CSCub07868

  Symptom: The **show controller pos pm** command does not display the correct SFP line type for 'SPA-1XOC12-POS'.

  Conditions: Line type is shown as LONG MM for all SFPs in show controller pos pm.

  Workaround: `show hw-module subslot x/y transceiver #port idprom brief IDPROM for transceiver POS0/1/0: Description = SFP or SFP optics (type 3) Transceiver Type: = OC12 LR-1/STM4 L-4.1 (12).`

- CSCub07931

  Symptom: White noise after Transfer completion.

  Conditions: SRTP-RTP xcoder is allocated on CUBE. Version 15.2(3)T1.

  Workaround: There is no workaround.

  CSCub13457

  Symptom: Memory Leak seen at xcode_associate_local_stream.

  Conditions: Leak could be seen for SIP-SIP transcoded call with mid-call UPDATE (with SDP) pass-through or UPDATE-to-ReINVITE cases.

  Workaround: Disable UPDATE, instead use ReINVITE for mid-call renegotiations.

- 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.

- 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: There is no workaround.

- CSCub18086

  Symptom: FlexVPN IKEv2 adding ipv4 address and not adding ipv6 address to the tunnel interface.

  Conditions: Unassigned local pool on client.

  Workaround: There is no workaround.

- CSCub28997

  Symptom: Overlord crashes with 2000 crypto sessions (4000 IPSec SAs) upon repeatedly clearing and reestablishing the SAs.

  Condition: The box is configured with 1K VRFs and 1K Virtual templates. And the crypto sessions are repeatedly cleared/reestablished.

  Workaround: There is no workaround.

- CSCub33119

  Symptom: **sh pl software interface fp active name interfacexxx ip reassembly?** command doesn't display reassembly parameter correctly.

  Conditions: When the router is not configured reassembly max-reassembly value, it is using its default value 16. in this case, ios **sh ip reassembly gigabitEthernet 0/0/0** will display this value correctly, but binos (**show platform software inter fp active name xxx ip reassembly**) will not. Workaround: There is no workaround.

- CSCub34318

  Symptom: Some of SIP calls between Cisco IOS Voice gateway and a remote SIP UA that is behind a NAT router may experience audio issue (one way audio) if a private IP address is being advertised by the remote site for the media connection.

  Conditions: When Cisco IOS Voice gateway has a peer SIP UA that is behind a NAT router, and a private IP address is being advertised during the call setup by the remote side, you may need to enable, on the IOS Voice Gateway, support for Symmetric NAT traversal using "nat symmetric check-media-src" command to have the voice gateway to learn the media address and port from the first incoming RTP packet. But two consecutive 180 responses received by the IOS Voice gateway (during call setup) with different "To:" tags (what is a normal behavior of a SIP Proxy), is breaking this support for "SIP NAT symmetric" feature. And you will experience one way audio issue even though "nat symmetric check-media-src" is configured.

  Workaround: There is no workaround.

- CSCub35268

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

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

Workaround: There is no workaround.

- CSCub39131

  Symptom: Packets are dropped.

  Conditions: 5cps basic sip call.

  Workaround: Reduce the traffic load from 5 CPS to 2 CPS.

- 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.

- 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.

- CSCub46841

  Symptom: CUBE reboot.

  Conditions: Under recording load.

  Workaround: There is no workaround.

- CSCub49291

  Symptoms: Static tunnels between hubs and spokes fail to rebuild.

  Conditions: The symptom is observed when you reload the hub on the DMVPN IPv6 setup with DPD on-demand enabled on all spokes.

  Workaround: There is no workaround.

- CSCub50350

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

Conditions: This symptom occurs due to the remote loopback configuration.

Workaround: There is no workaround.

- CSCub50601

  Symptom: Cube CME Call - Working with SCCP XCoding / Not Working with LTI.

  Conditions: HA Configuration exists on Cube.

  Workaround: Don't Configure HA.

- CSCub50695

  Symptom: The netflow data is fragmented when an IPv6 exporter is used.

  Conditions: The symptom occurs when:

  – An IPv6 exporter is used

  – A large amount of data is to be exported at once.

  Workaround: There is no workaround.

- CSCub50708

  Symptom: `call flow: PSTN--3rd party ---SIP--CUBE--SIP--3rd party--agent IOS version: c3900-universalk9-mz.SPA.151-3.T3 when CUBE receive multiple 183 session progress, for the 3rd 183 session progress <- the third 183 session progress -> PRACK 104 <-200 OK for INVITE ->ACK for INVITE -->REINVITE 105 <-200OK for PRACK 104 ->ACK 105`. The ACK for the PRACK has the wrong Cseq number. It should be 104 instead of 105.

  Conditions: CUBE receives multiple 183 session progress.

  Workaround: There is no workaround.

- CSCub51279

  Symptom: A Cisco ASR1k series router resets its FP with FW NAT feature combination.

  Conditions: A Cisco ASR1k series router resets its FP with FW NAT feature combination along with traffic.

  Workaround: There is no workaround.

- CSCub52943

  Symptom: When executing Media Forking with midcall codec change, memory leaks are found in Cisco ASR for CCSIP_SPI_CONTROL. After decoding, the memory leak is found to be for the function is_x_participant_sips() as it is not releasing the memory after allocated with some memory. This seems to be a side effect of one of the DDTS that was committed to Cisco IOS Release 15.3M&T (CSCtz96408).

  Conditions: This symptom occurs when executing Media Forking with midcall codec change.

  Workaround: The fix is done and is committed to Cisco IOS Release 15.3M&T.

- CSCub53856

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

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

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

- CSCub56064

  Symptom: Ping fails after doing EZVPN client connect if CEF is enabled.

  Conditions: This symptom is observed with the Cisco IOS Release 15.3(0.8)T image. This issue is seen only for a specific topology, where the in/out interface is the same.

  Workaround: There is no workaround.

- CSCub57913

  Symptom: The memory of ESP is exhausted due to continuous leak in the cpp_ui_pfr TDL messages.

  Conditions: This condition occurs when the **show platform hardware qfp active feature pfr** is used repeatedly.

  Workaround: There is no workaround.

- CSCub58775

  Symptom: The stand by RP of the Cisco ASR1000 routers might crash if the Stby-rp "cmand" core is written after ASR1013-PWR-DC replacement.

  Conditions: This issue occurs either after an OIR of a power-supply or when similar events occur.

  Workaround: There is no workaround.

- CSCub59275

  Symptom: Configuration of CT3 controller Serial interfaces does not match between standby RPs. Several error messages such as there are generated :

  %COMMON_FIB-4-FIBHWIDBMISMATCH: Mis-match between hwidb Serial1/0/1/2:0 (ifindex 634) fibhwidb Serial1/0/1/1:1 (ifindex 634) - appears on standby RP during controller configuration.

  IP addresses are assigned to wrong Serial interfaces. Due to mismatch of interfaces, during RP switchover traffic does not pass through.

  Conditions: This condition occurs when the CT3 SPA is configured on a dual RP router

  Workaround: There is no workaround.

- CSCub60278

  Symptom: OSPF neighbor cannot bring up over point to multipoint atm bundles.

  Conditions: This condition occurs when two Cisco ASR 1000 routers are directly connected with ATM pvc bundles, one end is point-to-point sub-interface and the remote is multipoint sub-interface. When you try to run OSPF over bundle, the OSPF neighbors bring up over point to multipoint atm bundles.

  Workaround: Change to P2P ATM interface.

- CSCub61637

  Symptom: Mid-call xcoder insertion does not happen when TCL app is involved in the call

  Conditions: TCL app initially connects a SIP trunk call to SCCP phone and later transfers to CUE-voice mail

  Workaround: Do not use TCL app or have same codec settings on either side of trunk

- CSCub62988

  Symptom: Cisco ASR 1000 routers crashes consecutively.

Conditions: This condition occurs on Cisco ASR 1000 routers with ESP10 with ios 15.2(2)S

Workaround: There is no workaround

- CSCub63146

  Symptom: No modem upspeed.

  Conditions: This condition occurs when modem pass through protocol based configured include g711/silence suppression in the RINGING/200 OK

  Workaround: Use SIP profile to strip "silence suppression off" in the incoming messges of the intial call setup

- CSCub63208

  Memory corruption detected in memory, when allocated for RTCP statistic

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

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

  Workaround: There is no workaround.

- CSCub64068

  Symptom: "CPPOSLIB-3-ERROR_NOTIFY F0: cpp_cp: cpp_cp encounters an error" log message with tracebacks. This results in a ESP crash or control plane or configuration events are not processed on the ESP.

  Conditions: This symptom is observed with a combination of ESP20 or ESP40 and CC40 installed on a Cisco ASR 1006 router or Cisco ASR 1013 router. This issue is observed when the CC40 does not have SPAs installed in bay 0 or 2 and bay 1 or 3.

  Workaround: If you have two or more SPAs installed in the CC40, ensure that there is a SPA in bay 0 or 2 and bay 1 or 3. If you only have one SPA installed in the CC40, there is no workaround.

- CSCub65151

  Symptom: The Cisco ASR 1000 CPP crashes when shutting down core facing MPLS interfaces on NPE

  Conditions: This condition occurs rarely.

  Workaround: There is no workaround.

- CSCub65380

  Symptom: when SIP gateway receives an INVITE with user=phone in the request URI, the prefix" " is removed from phone number. For example, when gateway receives the following INVITE INVITE sip: 1234567;npdi=yes@14.50.219.4:5060;user=phone SIP/2.0 It will route the call to 1234567, instead of 1234567

  Conditions: This condition is observed when user=phone in the request URI.

  Workaround: There is no workaround.

- CSCub66957

  Symptom: ESP40 Crash seen with 4% traffic on a basic LSM setup . Basic LSM setup of PE-P-PE.

  - 1 join for SM, 1 join for SSM, 1 join for Bidir. (Both v4 and v6)
  - Router is performing a tail end (Disposition) function.
  - Moment traffic hits the box, ESP 40 crashes. (4% of Gige line rate, 2% for v4 and 2% for v6)

  Conditions: ESP40 crashes when traffic passes through the router.

Workaround: Disabling LRE fixes the issue set platform hardware qfp active feature multicast v4 lre off set platform hardware qfp active feature multicast v6 lre off.

- CSCub68021

  Symptom: A **show interface** command on a SPA interface shows "0" for "unknown protocol drops", yet when the same interface is polled for ifInUnknownProtocols, a value is returned.

  Conditions: This condition is observed during normal polling.

  Workaround: There is no workaround.

- CSCub68200

  Symptom: FP may crash while flapping sessions with ISG services, or flapping the ISG services themselves.

  Conditions: This behavior might be seen on the Cisco ASR 000 routers 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 observed when such services are quickly added and removed from a subscriber.

  Workaround: There is no workaround.

- CSCub68814

  Symptom: CUBE sends response to reinvite from CVP through proxy, not respecting Via header of reinvite. Response should be sent directly back to CVP

  Conditions: SIP call routing from ITSP to CUBE to SIP Proxy to CVP. Initial transaction is handled through the proxy. With record route turned off the CVP sense reinvites directly to the CUBE, bypassing the proxy. The Via header of the reinvites indicated to send responses directly back to CVP. However the CUBE sends the responses to the proxy.

  Workaround: There is no workaround.

- CSCub69414

  Symptom: Traceback at FreeUInt64 on booting up router

  Conditions: An ASR 1006 router running mcp_dev towards XE38 On booting up the router seeing a traceback

  Workaround: The tracebacks are due to snmp-server enable traps entity-qfp mem-res-thresh. Disable the snmp-server enable traps entity-qfp mem-res-thresh.

- 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.

- CSCub70819

  Symptom: There is no way for customers to upgrade existing throughput licenses. (ex. from throughput_10g to throughput_20g)

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

  Workaround: The throughput value can be obtained by installing the corresponding exact throughput license.

- CSCub71981

Symptoms: The **show voice register pool on-hold brief** command displays the same number (for both phone number and remote number) when both local and remote phone are put on-hold.

Conditions: This symptom is observed when with Cisco IOS Release 15.3(8)T.

Workaround: There is no workaround.

- 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.

- 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.

- CSCub74279

  Symptom: While ringing, warm transfer committed which does not negotiate with video. Agent-1 complete transfer to Agent-2, while agent-2 is ringing and after sometime Agent-2 pick up the call.

  Conditions: This symptom is observed when:

  - Caller and Agent-1 had 2-way audio.
  - Agent-1 did a warm transfer. Caller puts on hold and Agent-2 is ringing.
  - Agent-1 complete the warm transfer. Still Agent-2 is ringing.
  - After sometime Agent-2 pick up the call.

  Workaround: There is no workaround.

- CSCub76384

  Symptom: In legacy call-park mechanism, when a call is parked and if the parkee hangs up while waiting for the parked call to be answered, the final party who dials the park slot DN hears MOH and is put on hold and is unaware that the parkee has dropped the call.

  Conditions: This symptom is observed in CME : 8 and 9 versions (tested till CME 9.0) IOS : 15.X (tested till 15.2(3)T1)

  Workaround: Add the following under "telephony-service" to move from legacy call-park mechanism: call-park system application.

- 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 1000 router 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.

- CSCub78299

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

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

Workaround: There is no workaround.

- CSCub79318

  Symptom: Codec changes spontaneously during mid-session without a RE-INVITE

  Conditions: This symptom occurs with the following conditions:

  - Fax passthrough is configured.
  - Codec negotiated is G711alaw, and changes to G729.

  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.

- CSCub79806

  Symptom: - H323 GW disconnects call due to pre-ACF notify

  A sample signaling flow: GK---(h323)----GW---(h323)---CVP <----SETUP------ <-----ARQ----- <----NOTIFY----- -----Disengage-> ------ACF---->

  Conditions: - Notification is received by the GW prior to the ACF

  Workaround: There is no workaround.

- CSCub80491

  Symptoms: A Cisco router may experience alignment errors. These alignment errors may then cause high CPU.

  Conditions: This symptom occurs as the alignment errors require using Get VPN. It is currently believed to be related to having the Get VPN running on a multilink interface, but this is not yet confirmed.

  Workaround: There is no workaround.

- CSCub80654

  Symptoms: Randomly, there is no audio if a call comes from the following call flow using G729: IP Phone -- CUCM -- ICT GK Controlled -- GK -- CME 9.1 -- Phone A and B If one of the phones in CME tries to GPickup the call randomly, it will have no audio. When this happens, if you check the codec directly in the phone, it is G711. However, when it works, it is G729. Everything is configured for G729. Even if you hard code the phone in CME to use G729, this issue will occur. This issue does not occur in CME 7.1.

  Conditions: This symptom occurs if a call comes from GK as G729 and CME 9.1 is being used.

  Workaround: Use CME 7.1 or enable fast start in CUCM Trunk by enabling the following check boxes:

  - Media Termination Point Required
  - Enable Outbound FastStart

- CSCub80710

  Symptoms: SSL handshake between Cisco VCS and the Cisco ASR fails if the Cisco ASR 1000 router is running Cisco IOS XE Release 3.7S. image

Conditions: This symptom occurs in a working setup, if the Cisco ASR is upgraded to Cisco IOS XE Release 3.7S, then SSL handshake and subsequently SIP-TLS calls start to fail. If in the same setup, the Cisco ASR is downgraded back to Cisco IOS XE Release 3.5S or Cisco IOS XE Release 3.4.4S, then the calls work (without requiring any additional changes).

Workaround: There is no workaround.

- CSCub81374

  Symptom: ASR1001 Feature Navigator does not show correct image to license mapping

  Conditions: This condition is observed for ASR1001 ordering with or without licenses.

  Workaround: There is no workaround

- CSCub81489

  Symptom: **show tech-support out** is not displayed intermittently.

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

  Workaround: Execute **show log** or any other **show tech-support** command, out is displayed again.

- CSCub82275

  Symptom: Cisco ASR 1000 Routers may experience reloads on the ESP module due to a CPP driver fault during an in-2-out NAT translation. .

  Conditions: Issue has been observed with IOS 15.2S, but not in 15.1S when NAT is enabled. No other requirements known.

  Workaround: Disable NAT or downgrade to a 15.1 release.

- CSCub83071

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

  Conditions: This condition is observed when configure mediatrace and RP switchover is performed twice.

  Workaround: There are two workarounds:

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

- CSCub83960

  Symptom: After the second RP switchover, mcast traffic stop forwarding by PE.

  Conditions: mVPN topo, during mcast traffic sending, do RP switchover on PE1.

  Workaround: Using Clear ip mroute * to make the global MDT mroute re-built can restore mcast traffic before or after the second switch-over.

- 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.

- CSCub84204

  Symptom: GTPv0 request dropped and failed to create session

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

Workaround: There is no workaround.

- CSCub85608

  Symptom: ASRNAT address leak may occur. This will show a larger number of allocated addresses in **show interface nat stat** command, then the translations that exist for that address via the **show ip nat trans** command

  Conditions: This issue only occurs when a dynamic route-map configuration is used and the NAT sub-drop code ESP_CREATE_FAIL is incrementing (i.e. there must be ESP traffic).

  Workaround: The leaked addresses can be reclaimed periodically by executing a **clear ip nat trans *** command, but that will be disruptive to users so this task should be schedule during off-hours.

- CSCub86791

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

  Condition: 1RU platform XE3.8 installed. maximum flows set to 750000 you have traffic which contains flows higher than 750000

  Workaround: There is no workaround.

- CSCub86827

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

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

  Workaround: Remove the after hours configuration .

- 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.

- CSCub89150

  Symptom: pw with backup

  Conditions: switch between active/standby pw

  Workaround: reload the boxes

- CSCub89157

  Symptom: GTP: CPC response message is dropped.

  Conditions: This condition occurs when cause is not equal 128.

  Workaround: Resend the messages.

- CSCub89194

  Symptom: On boot, the group member registers KS twice.

  Conditions: This condition is observed only during bootup.

  Workaround: There is no workaround.

- CSCub89711

  Symptoms: The **atm** keyword in the **show** command disappears after a SPA power shut.

  Conditions: This symptom occurs when a SPA card is powered shut and is brought back up using the **no** form of the previous command.

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.

- CSCub91150

  Symptom: Cannot ping SBC interface from ASR 1000 Router

  Conditions: This condition is observed when

  – SBC interface created with netmask /32

  – SBC activated

  Workaround:

  – Deactivate SBC

  – Delete SBC interface and re-create it again.

- CSCub91178

  Symptom: ALG FTP44 does not work, fails to establish data path.

  Conditions: This issue occurs under the following 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 is 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 .

- CSCub91815

  Symptom: Certificate validation fails with valid certificate.

  Conditions: This symptom is observed during DMVPN setup with an empty CRL cache. This issue is usually seen on the responder side, but the initiator can also show this behavior.

  Workaround: There is no known workaround.

- CSCub93048

  Symptom: NHRP error message should indicate node IP that triggers the Error Syslog message format is changed to include the trigger source, source NBMA and destination addresses.

  Example: %NHRP-3-PAKERROR: Received Error Indication from 10.0.0.2, code: administratively prohibited(4), (trigger src: 10.0.0.1 (nbma: 172.16.1.2) dst: 192.168.2.1), offset: 0, data: 00 01 08 00 00 00 00 00 00 FE 00 68 F4 03 00 34

  Conditions: This condition is observed when NHRP error indication is received on the box.

  Workaround: There is no workaround.

- CSCub93228

  Symptom: Traffic not passing even it matches the filter conditions are met.

Conditions: This condition in observed when IPv4 and IPv6 co-exist in the interface configuration and with FW NAT configuration.

Workaround: Instead of using pre-natted source address in ACL, use post-nat source address.

For example, 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 :

```
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
```

- CSCub93496

  Symptoms: One-way video from CTS-1000 to TS-7010 is seen in the following topology: CTS-1000 (v1.9.1) >>> CUCM 8.6.2aSU2 >>> CUCM 9.0 >>> CUBE 15.1.2T (2811) >>> CUBE 15.1.4M4 (2951) >>> CUCM9.0 >>> VCS X7.1 >>> TS-7010 2.2

  Conditions: This symptom occurs when SDP Passthrough mode on CUBE is used.

  Workaround: RTP payload types 96/97, which are associated with fax/faxack need to be remapped to some other unused values.

- CSCub94825

  Symptoms: After Cisco IOS XE bootup, there are no static reverse routes inserted as a result of applying/installing and HA crypto map. The same issue is present on the HSRP standby device, namely, the static RRI routes will not get installed in case a failover occurs. The **show cry map** command can be used to verify that RRI is enabled. The **show cry route** command can be used to determine if RRI has happened and if it has been done correctly.

  Conditions: This symptom is observed with the following conditions:

  – Cisco IOS XE Release 3.5 up to Cisco IOS XE Release 3.7 - VRF-aware IPSec with stateless HA and static RRI - IPv4 Workaround: Removing and reentering the **reverse-route static** command into the configuration will actually trigger the route insertion.

    Problem Description After IOS-XE bootup, there are no static reverse routes inserted as a result from applying/installing and HA crypto map. Same issue is present on the HSRP standby device, namely, the static RRI routes will not get installed in case a failover occurs. show cry map.

  – can be used to verify that RRI is enabled show cry route - can be used to determine if RRI has happened and if its been done correctly Conditions IOS-XE 3.5 - 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 will actually trigger the route insertion.

- CSCub96558

  Symptom: Phone calls to a Directory Number (DN) on a Cisco Communications Manager Express (CME) system gets continuous ringback tone instead of forwarding to a voicemail number or any other configured "call forward" destination.

  Conditions: The problematic DN is a "shared line" between a SIP phone and a SCCP phone registered to the same Cisco CME system. Both SIP and SCCP phones that have the "shared line" are configured with the same "call forward' parameters. The CME system version is 9.0 or higher. The SCCP phone is "unregistered" from the CME system during the problem occurrence.

  Workaround: Since the problem only happens when the SCCP phone is "unregistered" from the CME system, possible workarounds would be:

  - Diagnose and fix the "unregistration" issue on the SCCP phone
  - Configure the "shared line" on another SCCP phone that is registered and reset the phones

- CSCub96576

  Symptom: Reload may occur when removing static rmap mapping.

  Conditions: On ASR1k NAT very rarely reload may occur when removing static rmap mapping

  Workaround: There is no workaround.

- CSCub97641

  Symptom: Netflow was tested on NAT CGNmode, abnormal Netflow log was found . But no issues were found for the default mode .

  Conditions: configure 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.

- CSCub98177

  Symptom: In the ASR1K that has a LAC running IOS XE RLS3.5.2, disconnects the PPP session by TermReq without any reason, each time in the **show pppoe stat** incrementing the **SSM DISCONNECT**.

  Conditions: This symptom occurs in the SSO mode, RP switchover.

  Workaround: There is no workaround.

- CSCub98357

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

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

  Workaround: Disable 'ocsp disable-nonce'.

- CSCub99205

  Symptom: Mod F: Shaper becomes inactive when policy-map rem/add back on sub-interfaces

  Conditions: This issue occurs each time on rem/add on sub-interface.

  Workaround: Changing shaper value reactivates shaper.

- CSCub99216

  Symptom: With DMVPN phase2, the DMVPN hub is not responding to a resolution request for an address that the hub has an authoritative cache entry. Instead it's forwarding the request along the routed path.

  Conditions: - This problem is observed in a DMVPN phase 2 deployment environment, where the hub router is configured with **no ip nhrp cache non-authoritative** command. - XE 3.6 and above.

  Workaround: There is no workaround.

- CSCub99756

  Symptoms: The Cisco ASR 1000 router running Cisco IOS Release 15.2(4)S acting as a GM in a Get VPN 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 symptom is observed only in Cisco IOS Release 15.2(4)S.

  Workaround: There is no workaround.

- CSCub99778

  ASR1K GETVPN GM does not attempt registration after reload interface up

  Symptoms: The Cisco ASR 1000 router being GM in a Get VPN deployment fails to start GDOI registration after a reload.

  Conditions: This symptom occurs when running Cisco IOS Release 15.2(4)S. The following error is displayed in the **show crypto gdoi** command output after reload. Registration status: Not initialized.

  Workaround: Use an EEM script to issue **clear crypto gdoi** command some time after boot time or issue this manually.

- CSCuc00465

  Symptom: configured permit-error, for 3GPP RLS7&8 req/resp, sessions are created, but for those unknown/unwanted IE, gtp counter does not work correctly.

  Conditions: This condition is observed when permit-error is turned on.

  Workaround: There is no workaround.

- CSCuc00658

  Symptom: Unable to ping direct connected peer ip address.

  Conditions: This issue occurs under the following conditions:

  - config ip reassembly on sub interface
  - configure ipv6 reassembly on the same sub interface
  - no sub interface

  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.

- CSCuc01368

  Symptom: This is issue introduced in skyrise as part of a feature. This a display issue due to space length defined for displaying ipv6 addresses

  Conditions: Media addresses being used is IPV6 and when **show voip rtp connections** is run.

  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: Cisco ASR 1000 router is configured as L2TP LNS. At that time, EssUnsupPktType drop counter is incremented.

Workaround: There is no workaround.

- 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.

- CSCuc03389

  Symptom: traceback message can be observed on the voice gateway %SDP-3-SDP_PTR_ERROR: Received invalid SDP pointer from application. Unable to process. -Traceback= 0x637B4F10z 0x61ADC2B4z 0x61A4886Cz 0x61AD6AC8z 0x619919BCz 0x6199A6C8z 0x61B30364z 0x61B3082Cz 0x63A7BCACz 0x63A7BC90z

  Conditions: Router with IOS 15.1(3)T4

  Workaround: There is no workaround.

- CSCuc03831

  Symptom: During system shutdown, occasionally the system will reboot, with a soft reset indication shutdown, before the system reaches a safe reboot state.

  Conditions: This condition is observed when the system is trying to shutdown and system reaches an error state. the system unexpectedly reboots with a soft reset indication, but no core or tracefiles are saved.

  Workaround: There is no workaround.

- CSCuc04061

  Symptom: When CUCM sends a single digit ASR is sending multiple NTE events as expected however the Marker bit is incorrectly set to TRUE most of them.

  Conditions: ASR1006 running 15.2(2)S1 is configured as an MTP.

  This problem is observed on the release 3.6.1 (asr1000rp1-adventerprisek9.03.06.01.S.152-2.S1) image.

  The release 3.4.3 (asr1000rp1-adventerprisek9.03.04.03.S.151-3.S3.bin) image is not affected.

  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: This symptom is not caused by any specific conditions.

  Workaround: As this is a corner case situation, un-shutting and shutting down the interface may resolve the issue.

- CSCuc05174

  Symptom: ESP Crashes

  Conditions: Configuration results in exhaustion of CPP external memory

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

- CSCuc05660

Symptom: ttl in CNAME record is reset

Conditions: DNS CNAME record

Workaround: There is no workaround.

- CSCuc05671

  Symptom: The console reports "[aom]: (ERR): Unable to find async context for AOM" and traceback.

  Conditions: 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 command "call-policy-set copy source x destination y", the na-src-name-anonymous-table is not copied.

  Conditions: If you copy the policy to a set number that did not 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.

- CSCuc07317

  Symptom: **Show controller pos pm** command does not show correct SFP line type for All POS SPAs

  Conditions: Line type is shown as LONG MM for all SFPs in show controller pos pm frp Sphinx/POS and SHORT SM for Iguana/Ninja

  Workaround:

```
show hw-module subslot x/y transceiver #port idprom brief IDPROM for transceiver
POS0/1/0:  Description                          = SFP or SFP optics (type 3)
Transceiver Type:                      = OC12 LR-1/STM4 L-4.1 (12)
```

- CSCuc08061

  Symptom: IPv6 DMVPN spoke failed to re-build tunnels with hubs.

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

  Workaround: Reboot the spoke.

- CSCuc08964

  Symptom: IOS PKI server keeps updating CRL list even if PKI server is shut down. Found in 15.1.4.M, but may be more wide spread.

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

  Workaround: Block access to CRL Distribution point so PKI server will not be able to upload updated CRLs.

- CSCuc09772

  Symptom: ISR running CME with AFW may experience bus error crashes and spurious accesses during call disconnect.

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

  Workaround: There is no workaround.

- CSCuc10081

Symptom: ISSU/ISSD would be failed.

Conditions: Always

Workaround: There is no workaround.

- CSCuc11275

  Symptom: PSTN user cannot hear the MOH when the call is put on hold.

  Condition: If a call is put on hold after the previous call is parked using PARK softkey, the PSTN user cannot hear the MOH.

  Workaround: The following workarounds are available:

  - Use FAC code to park the call.
  - Seize this DN and then release it to reset the park flag after parking a call.

- CSCuc11853

  Symptom: T1 controller will stay DOWN after switchover.

  Condition: This symptom is seen when SATOP is configured on T1.

  Workaround: Do a shut and no shut.

- CSCuc12685

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

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

  Workaround: There is no workaround.

- CSCuc14204

  Symptom: IOS PKI certificate enrollment fails due to collision with another enrollment request.

  Condition: IOS PKI auto-enrollment Multiple trustpoints are configured and try to enroll at same time. See error: CRYPTO_PKI: Failed to send the request. There is another request in progress.

  Workaround: Use manual enrollment. Use different re-enrollment percentages on each trustpoint.

- CSCuc15854

  Symptom: SRTP - RTP fallback failure - CUBE sends back both 488 and 503

  Condition: For a SRTP - RTP transcoding failure scenario, CUBE sends back both 488 and 503 response codes. It should reject the call with only 503 with the correct Warning Header.

  Workaround: There is no workaround.

- CSCuc16623

  Symptom: After changing the grandparent shape rate via ancp, traffic is not shaped to the new rate.

  Condition: PPPoE model F QoS. Via ancp, change the grandparent shape rate.

  Workaround: There is no workaround.

- CSCuc20045

  Symptom: The maximum configurable PBHK (Port Bundle Host Key) source interfaces on an ASR1K router is random and could be as low as 1. Here is a sample error message seen on a customer's ASR1K router when adding 83rd source interface for PBHK: PortBundle: Unable to add source IP into list PortBundle: Command failed PortBundle: allowed number of source IPs: 82

  Condition: Configure multiple PBHK source interfaces on an ASR1K router.

  Workaround: There is no workaround.

- CSCuc22348

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

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

  Workaround: There is no workaround.

- 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.

- CSCuc22942

  Symptom: Show version may report reload due to address error. Example: System returned to ROM by address error at PC 0x7F10BB0, address 0x4E1B383C at 23:46:01 EDT Mon Sep 10 2012 System restarted at 18:17:48 EDT Thu Sep 13 2012 System image file is "flash:c2951-universalk9-mz.SSA_8_5_ES2.1" Last reload type: Normal Reload Last reload reason: address error at PC 0x7F10BB0, address 0x4E1B383C This bug happens within IOS internal. It is not a common and at the same time, not a a rare occurrence.

  Condition: Platform independent. Seen usually in 29xx and 39xx class routers. Originally seen in 15.2(2)T and 15.2(4)M release. Feature that need to be active for this crash to happen: Music on hold should be actively in use.

  Workaround: There is no workaround. If you suspect that you are affected by this OR if you are proactively researching for known bugs to side-step, kindly engage your Account Team or your Advanced Services Team for guidance. Releases that have the fix include: 15.2(2)T3, 15.2(4)M3 and later releases.

- CSCuc24741

  Symptom: buffer overflow in **opssl_parser** corrupts OPSSLContext when all cipher suites were selected

  Condition: This symptom occurs on working setup, when all the cipher suites were selected at openssl layer. This issue is observed from xe37 onwards.

  Workaround: Instead of selecting all cipher suites, select required cipher suite.

- 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.

- CSCuc25529

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

  Condition: 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.

  Condition: On clear ip nat translations **vrf** *vrf-name**.

Workaround: Use clear ip nat trans * This issue exists only on Cisco IOS XE Release 3.7.1S.

- CSCuc26434

  Symptom: RP information is not learned when Auto-RP is configured for customer domain and the MA and RP candidate are on different PE.

  Condition: MA and RP candidate are on different PE.

  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.

- 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.

- CSCuc30500

  Symptom: The following features: NBAR, FNF (AVC), Seawolf (FME), and Lhotse (AppNav)) may appear as being properly activated where as, they are not.

  Condition: CFT infra that above listed features are not properly initialized.

  Workaround: There is no workaround.

- CSCuc31692

  Symptom: ASR1K ucode crashes with scaled MLPPP configuration with sustained high data rates across most bundles.

  Condition: Highly scaled MLPPP configuration with sustained high data rates across most bundles. Problem has only been seen with the ESP40. Likelihood of encountering this issue is lesser because this issue has only been seen in a lab environment under extremely high data rate conditions.

  Workaround: There is no workaround.

- CSCuc31725

  Symptom: CUBE fails to resolve the configured DNS through a query when the SRV query fails.

  Condition: This symptom occurs when running Cisco IOS Release 15.3(0.11)T.

Workaround: Use DNS SRV records for SIP servers.

- CSCuc31761

  Symptom: Router crashes when removing GDOI groups.

  Conditions: KS has 100 GDOI groups being configured.

  Workaround: There is no workaround.

- CSCuc34574

  Symptom: 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.

- 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 (i.e. the original fragment size configuration is retained). The IOS **show ppp multilink** command indicates that the new fragment size was applied but, in fact, the new fragment size may not yet be active.

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

- CSCuc33214

  Symptom: The PADI drops statistics shown in show interafces are not cleared.

  Conditions: When there are PADI drops on any of the ATM interfaces, they are displayed in show interfaces. And, these are not cleared even after doing clear stats.

  Workaround: There is no workaround.

- CSCuc34315

  Symptom: ASR crashes with fman_fp while unconfiguring in PBR scalability test.

  Conditions: After the scalability test is performed with 1024 intefaces, crash is observed.

  Workaround: There is no workaround.

- CSCuc36464

  Symptom: Traffic check fails for user-defined classes with HQoS policy.

  Conditions: This condition occurs on sending traffic from ixia.

  Workaround: There is no workaround.

- CSCuc36469

  Symptoms: Crash is observed when removing the **crypto call admission limit ike in-negotiation-sa** *value* configuration and clear crypto sessions, which triggers a connection from all the clients burdening the server and forcing it to crash within few seconds.

Conditions: This symptom happens only when 150 connections simultaneously try to establish connection with the head-end EzVPN server.

Workaround: Configure **crypto call admission limit ike in-negotiation- sa** *20* when scaling to 150 tunnels.

- CSCuc38440

  Symptom: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED messages along with tracebacks are seen.

  Conditions: This symptom happens while configuring or unconfiguring the match message-id under class-map.

  Workaround: There is no workaround.

- CSCuc38911

  Symptom: Observed *(ERR): INTF: DELETE failed* trace log.

  Conditions: While creating Virtual Template Interface to test the L2TP scalability enhancements.

  Workaround: There is no workaround.

- CSCuc39469

  Symptom: Unable to monitor the second power supply that is just inserted into the ASR 1001 Router.

  Conditions: Insert the second power supply to the up and running ASR 1001 Router.

  Workaround: Make sure all power supplies are inserted before booting up the ASR 1001 Router.

- 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.

- CSCuc40585

  Symptom: Ucode crashes when the GTP AIC inspects the packets.

  Conditions: GTP AIC is configured.

  Workaround: There is no workaround.

- CSCuc40912

  Symptom: Stale objects are seen on RP SWO.

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

  Workaround: There is no workaround.

- CSCuc41243

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

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

  Workaround: There is no workaround.

- CSCuc43943

Symptoms: A Cisco ASR 1000 hub on dual-hubs causes DMVPN crash. This issue is only seen in Cisco IOS XE Release 3.9S.

Conditions: This symptom is observed with shut or no shut of the tunnel interface.

Workaround: There is no workaround.

- CSCuc44071

  Symptom: GRE keepalives are going out unencrypted if the Tunnel interface is in *up or protocol down* state.

  Conditions: This symptom occurs under the following conditions:

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

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

- CSCuc45528

  Symptoms: Leaks are seen at nhrp_recv_error_indication.

  Conditions: This symptom occurs only when the fix of CSCub93048 is present in the image.

  Workaround: There is no workaround.

- 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.

- CSCuc46352

  Symptom: One-way audio when using anti-trombone on a CUBE for a inbound call that is call forwarded back to the ITSP. After the call is forwarded, the CUBE never sends a Re-INVITE to the calling party to change the IP address from it's own IP to the IP of the ITSP. Therefore, the calling party doesn't get any audio. Whereas, the forwarded party hears the calling party fine.

  Conditions: **media anti-trombone** command is configured under *voice service voip*.

  Workaround: There is no workaround.

- CSCuc47356

  Symptoms: Static routes are not getting removed.

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

  Workaround: Remove the ACL before removing the SA.

- CSCuc47399

Symptoms: IKEv2 STOP Accounting records show wrong counters for packets/octets, when the sessions are locally cleared using **clear crypto sa** command or **clear crypto session** command on ASR 1000 Routers.

Conditions: This symptom is observed with latest Cisco IOS XE Release 3.8S images when IKEV2-Accounting 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.

- CSCuc48884

  Symptom: Cannot make more than 4000 CUBE calls with the default configuration, and this can be a limitation for HA as well.

  Conditions: Trying to make more than 4000 CUBE calls.

  Workaround: In most cases, multiple media-address ranges can be configured, though this may not work for HA.

- CSCuc49319

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

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

  Workaround: There is no workaround.

- CSCuc49386

  Symptom: Traceback is seen @ crypto_gdoi_gm_wavl_show_members_in_group.

  Conditions: Execute the **show crypto gdoi ks members** *A.B.C.D* command on GETVPN group member.

  Workaround: There is no workaround.

- CSCuc50498

  Symptom: cpp_cp_svr crash is observed.

  Conditions: This symptom occurs on attaching service-policy to member link with port-channel configured.

  Workaround: There is no workaround.

- CSCuc51076

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

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

  Workaround: There is no workaround.

- CSCuc53085

  Symptom: When the peer's public key has outlived its usefulness, it will be marked for deletion and upon the next time, we search the public key cache, all peer public keys that are marked for deletion are removed. In the case of this defect, it has been observed that, after performing a manual CRL update (**crypto pki crl request** *TrustPoint*) whatever the content of the crl response, the router deletes keys according to the following sequence: 10 keys, next time 6 keys, then next time 4 keys and so on, i.e. 2/1/0. This occurs whatever the amount of revoked certificates inside the updated crl

and it occurs also when the crl content does not change between different requests, i.e. when no certificates were revoked. So, the amount and number of keys to be deleted follows a pattern but the choice of key to be deleted is random. There is no negative impact on operation.

Conditions: Manual CRL update on a device running IOS 15.2(03)T. CRL caching is enabled.

Workaround: There is no workaround.

- CSCuc53349

  Symptom: In ASR CUBE-ENT platform, the **show voice call rate table** command displays the call per second (cps) information in histogram instead of tabular format.

  Conditions: None.

  Workaround: Use **show call history stats cps table** command instead. This command is available from Cisco IOS XE Release 3.8.

- CSCuc54220

  Symptoms: The SVTI always-up feature is broken.

  Conditions: This symptom occurs in clear and rekey cases.

  Workaround: Use **shut** and **no shut** commands.

- 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.

- CSCuc56259

  Symptoms: A Cisco 3945 that is running 15.2(3)T2 and running as a voice gateway may crash. Just prior to the crash, these messages can be seen: %VOIP_RTP-6-MEDIA_LOOP: The packet is seen traversing the system multiple times and Delivery Ack could not be sent due to lack of buffers.

  Conditions: This happens when a media loop is created (which is due to misconfiguration or some other call forward/transfer scenarios).

  Workaround: Check the configurations for any misconfigurations, especially, with calls involving CUBE and CUCM.

- CSCuc56895

  Symptom: Incorrect Profile trunk-route 4 is getting configured when different profile trunk-route is configured under Voice service saf.

  Conditions: Observed this issue in 15.3(0.13)T in c3945 platform.

  Workaround: There is no workaround.

- CSCuc57822

  Symptoms: The NBAR classification granularity reduced for some protocols or some protocols may be classified as unknown.

  Conditions: This symptom is observed when the following command is executed: **test platform hardware qfp active feature nbar function sui_gmc_show_chunks_brief**. If the *errors?* column has a non-zero value, it is most 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, perform 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. Reload 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**

- CSCuc57882

  Symptom: High CPU on the 2911 router causing voice-ports going from S_CONNECT/S_TRUNKED to -/S_TRUNK_PEND after a few hours. This is an LMR deployment (Hool and Hooter config) Call flow: ========== Recording server (E&M port) <------- (E&M port) 2911 <--------IP link--------(((multicast source --application)))

  Conditions: The High CPU was seen with the following IOS versions: c2900-universalk9-mz.SPA.152-4.M1.bin c2900-universalk9-mz.SPA.151-4.M2.bin 151-3.T4.bin

  Root Cause Of The Issue: In the above IOS versions, the issue was observed in the udp_checksum() routine, which gets invoked in this case as the other endpoint is sending the checksum. Currently, the behavior is such that when it receives UDP checksum in incoming packet, it will try to compute it. Thereby, leading to the High CPU errors and causing the PVDMs to crash, which leads to the voice ports going to S_CONNECT/S_TRUNKED to -/S_TRUNK_PEND after a few hours.

  Workaround: The following workarounds are available:

  - Make sure that udp checksum is disabled on the other endpoint sending the packet to us.
  - Have an image ready which basically ignores the udp checksum in the incoming packet, if the udp checksum is not important. The image was provided by the DE.

- CSCuc58513

  Symptom: Fp reload.

  Conditions: ALG traffic with ACL limit configuration.

  Workaround: Remove ACL limit configuration with ALG traffic.

- CSCuc59991

  Symptom: Traceback may appear on applying or removing Seawolf configuration.

  Conditions: In very rare condition of massive applying or removing Seawolf configuration sequence, the traceback may appear.

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

- 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.

- CSCuc60509

  Symptoms: A Cisco 2951 that is running Cisco IOS Release 15.2(1)T1 may have a processor pool memory leak in CCSIP_SPI_CONTROL.

  Conditions: The issue is seen when CUBE receives a PUBLISH request. At customer site, the issue was seen due to incorrect SIP trunk configuration, which resulted in PUBLISH requests to be sent to CUBE instead of CUSP.

  Workaround: Correct the SIP Trunk configuration so that PUBLISH requests are not sent to CUBE.

- CSCuc61244

  Symptom: BFD flaps.

  Conditions: Configure hardware BFD and configure egress ACL.

  Workaround: Change the hardware BFD to software mode.

- CSCuc61956

  Symptom: Agent Stats corrupted on agent reset.

  Conditions: Set timezone other than UTC on the CME router and reset the agent in EHG.

  Workaround: There is no workaround.

- CSCuc62078

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

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

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

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

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

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

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

- CSCuc62212

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

  Conditions:

  Workaround: There is no workaround.

- CSCuc62409

  Symptom: Pseudotime skew between Secondary key servers and Primary key server.

  Conditions: Clear crypto GDOI on the primary key server. It has been seen in 15.2(4)M1 but not in 15.1(4)M1.

  Workaround: Clear crypto GDOI on all devices.

- CSCuc63246

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

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

  Workaround: There is no workaround.

- CSCuc63696

  Symptom: Sometimes, cable detect test reported false (not connected) test result on FXOGS.

  Conditions: Cable detect test and incoming call to FXOGS are running at the same time.

  Workaround: There is no workaround.

- 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.

- CSCuc65437

  Symptom: cpp_cp_svr crash is seen.

Conditions: This symptom occurs on removing service-policy from main int.

Workaround: There is no workaround.

- CSCuc65609

  Symptom: During SIP attack, NAT causes ESP lock-up.

  Conditions: SIP registration attack.

  Workaround: Using ACL to block SIP attack.

- CSCuc66821

  Symptom: Remote-Party-ID is missing in the SIP Re-Invites.

  Conditions: When using newer CUBE version 8.7.

  Workaround: Currently not identified.

- CSCuc67468

  Symptom: **show platform h q a f nat data dynbin** command output gets into a loop.

  Conditions: When executed on ASR 1000 Routers.

  Workaround: Use **show ip nat trans** command and it's filters for showing this information

- CSCuc68743

  Symptoms: A crash occurs while running CME smoke regression.

  Conditions: This symptom is observed while running CME smoke regression.

  Workaround: There is no workaround.

- CSCuc69095

  Symptom: When cpp_fm_vmr_ops_execute_OPTIMIZE( ) function queries the TCAM manager for number of free entries in TCAM, then cpp_fm_free_tcam_entry_query( ) throws an error sometimes.

  Conditions: This is always invoked for all the configurations that are attached.

  Workaround: A running count to keep track of free entries in TCAM has been implemented. This solution might not work for a configuration whose size is as big as the size of TCAM.

- 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.

- CSCuc70310

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

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

  Workaround: There is no workaround.

- CSCuc70578

  Symptom: While clearing the counters, we are seeing the error message. %IOSXE-3-PLATFORM: R0/0: kernel: /scratch/mcpre/BLD-BLD_V153_1_S_XE38_THROTTLE_LATEST_20121015_080026/os/linux/drivers/binos/i2c/psmcu/psmcu_main.c:read_from_psmcu (line 185): i2c_smbus_read_byte() returned -110. Other potential errors: %IOSXE-3-PLATFORM: R0/0: kernel: /auto/mcpbuilds13/release/03.08.00.S/BLD-03.08.00.S/os/linux/drivers/binos/i2c/psmcu/psmcu_main.c:read_from_psmcu (line 175): MCU set pointer command failed, -5.

  Conditions: Error message should not been seen, while clearing the counters.

  Workaround: There is no workaround.

- CSCuc71379

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

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

  Workaround: There is no workaround.

- 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.

- CSCuc72643

  Symptom: Memory leak.

  Conditions: periodic.

  Workaround: There is no workaround.

- CSCuc73677

  Symptoms: RSA keys are not generated correctly.

  Conditions: This symptom occurs when you first clear the RSA keys that are already generated on the router, and then generate the RSA keys.

  Workaround: There is no workaround.

- CSCuc73993

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

  Conditions: This symptom occurs only when there is a very large PPS in the single flow traffic and when NBAR is enabled

  Workaround: There is no workaround.

- CSCuc74857

  Symptom: NAT address pool exhaustion with high DNS traffic.

  Conditions: Payload addresses in DNS PTR record NATed 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: The following workarounds are available:

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

- CSCuc75142

  Symptom: Ucode crash when h323 ALG traffic passed through router.

  Conditions: This symptom is seen with ALG traffic.

  Workaround: Remove HSL logging. Problem is not seen.

- CSCuc75480

  Symptom: Show call active video compact command doesn't show any active video calls while testing EO-EO Secure Video Call over CUBE when SDP PassThru is enabled.

  Conditions: This symptom occurs on running with IOS version- 15.3(0.14)T.

  Workaround: There is no workaround.

- CSCuc76130

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

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

  Workaround: There is no workaround.

- CSCuc76298

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

  Conditions: This crash is seen in the following scenarios:

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

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

- CSCuc76670

  Symptom: 2X1GE-SYNCE (metronome) SPA does not boot on a 2RU (Cisco ASR 1002).

  Conditions: This symptom is observed from Cisco IOS XE Release 3.7.0S onwards, when the 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

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

- 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 symptom is observed when ZBF debugs are enabled.

  Workaround: Do not enable ZBF debugs with **detail** or **drop** keywords for all traffic. Instead, enable ZBF debugs only for the traffic you like to debug. For more information, See CSCtf45361.

- CSCuc78499

  Symptom: GTPv1 memory chunk leak.

  Conditions: This symptom is observed when the GTP AIC is configured

  Workaround: There is no workaround.

- CSCuc78702

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

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

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

- CSCuc79208

  Symptom: Error %Port <> is being used by system while configuring the static nat with the same ports for different IP addresses as shown below, we can sometimes get an error message **%Port 1720 is being used by system**: ip nat inside source list IP_PBX_MP_NAT_ACL_PUB interface Loopback12 overload ip nat inside source list IP_PBX_MP_NAT_ACL_SUB interface Loopback13 overload IP NAT inside source static tcp 161.92.7.42 1720 interface Loopback12 1720 ip nat inside source static tcp 161.92.7.43 1720 interface Loopback13 1720 This issue happens when we have nat with overload statements configured before we configure static nat for ports.

  Conditions: This happens if we have NAT with overload statements are configured first.
  Workaround: Remove all NAT statments and configure the static NAT before the NAT overload. (Note that we will get the failure message again at the reload time since the commands are nvgenned with the overload command first.)

- CSCuc79283

  Symptom: The nat64 map-t subcommands cannot be syntax checked when running **config check syntax**.

  Conditions: This applies only when the user runs **config check syntax** in the syntax check mode.

  Workaround: There is no workaround.

- CSCuc80725

  Symptom: VFR subblock remains without CLI IP virual-reassembly displayed.

  Conditions: This symptom is observed when NAT is enabled without VFR and VFR is re-enabled.

  Workaround: Do not enable the VFR manually.

- CSCuc81645

  Symptom: CPP crashes on overlord when the show command is executed.

  Conditions: There is no known conditions.

  Workaround: There is no workaround.

- CSCuc81650

Symptom: Ingress QoS policy-maps on frame-relay type interfaces do not correctly show QoS policy-map packet counters.

Conditions: This problem only occurs when egress QoS policy-maps are attached to a frame-relay sub-interface and to a frame-relay DLCI on that same sub-interface.

Workaround: Apply egress QoS policy-maps to only the frame-relay sub-inteface or to the frame-relay DLCI.

- CSCuc81993

  Symptom: IKEv2 framed route support on server is required.

  Conditions: IKEv2 framed route support on server is required.

  Workaround: There is no workaround.

- CSCuc82246

  Symptom: RTSP Timeout doesn't work on VXML GW when **Bargein** is set to N. IOS 15.1.M4 CVP 9.01 ICM 9.02. When the vxml GW receives the following, RTSP will not timeout <prompt bargein="false" cisco-maxtime="30s" cisco-typeaheadflush="false" > <audio src="rtsp://10.2.247.40/rtpencoder/moh.sdp" fetchtimeout="4s" /> When the vxml GW receive the following, RTSP will timeout at 30 seconds <prompt bargein="true" cisco-maxtime="30s" cisco-typeaheadflush="false" > <audio src="rtsp://10.2.247.40/rtpencoder/moh.sdp" fetchtimeout="4s" />

  Conditions: This symptom is observed when **Bargein** is set to N.

  Workaround: There is no workaround.

- CSCuc83104

  Symptoms: Path confirmation fails for blind transfer scenarios for both SIP Line and trunk-side scenarios.

  Conditions: This symptom is observed if **no supplementary-service sip refer** is configured.

  Workaround: Configure **supplementary-service sip refer**.

- CSCuc85002

  Symptom: Unexpected logs printed in the console during configuration. ***Oct 17 06:54:50.711: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F1: fman_fp_image: PORTLIST: (tcp/50.1.1.1 port 4096 - 5119) download to CPP failed *Oct 17 06:54:50.534: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image: PORTLIST: (tcp/50.1.1.1 port 4096 - 5119) download to CPP failed.**

  Conditions: This Symptom is seen when the configuration includes dynamic PAT (Port Address Translation) with the interface overload.

  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.

- CSCuc85319

  Symptom: RP is crashed.

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

Workaround: There is no workaround.

- CSCuc85807

  Symptom: Values of certain flows have incorrect jitter values when MMON is activated on non-video UDP traffic jitter.

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

  Workaround: There is no workaround.

- CSCuc87847

  Symptom: QFP crashes.

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

  Workaround: There is no workaround.

- CSCuc88112

  Symptom: Ucode crashes.

  Conditions: This symptom is observed while testing the **frf12** feature.

  Workaround: There is no workaround.

- CSCuc88175

  Symptoms: When a dynamic **cryptomap** is used on the Virtual Template interface, SAs are not created and the testscripts fail. This issue occurs because the **cryptomap** configurations are not added to the NVGEN, and hence there is no security policy applied on the Virtual Template interface.

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

  Workaround: There is no workaround apart from using tunnel protection on the Virtual Template interface.

- CSCuc88575

  Symptom: The following message can be seen on Cisco ASR routers which runs IOS-XE: FAILED: File [location]:[name] is not a valid consolidated package file.

  Conditions: Multiple conditions can lead to this error message. One of these is if the specified file doesn't exist at the path specified. The reason for failure is not clear.

  Workaround: There is no workaround.

- CSCuc89261

  Symptom: The router is crashed with ucode traceback.

  Conditions: This symptom occurs while adding **32 Service Node Group** under Service Context and removing them.

  Workaround: There is no workaround.

- CSCuc89646

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

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

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.

- CSCuc89958

  Symptom: Perf-mon flow timeout or expiry takes longer than expected

  Conditions: The functionality related to **timeout or expiry** of flows after media stop event seems to be taking longer than expected. The related configs are: - monitor params **interval duration <x**" and **timeout <y>**, under policy-map class submode or **- cache timeout .. <x>** and **history size <value> timeout <y>** under Perf-mon flow monitor config mode

  Workaround: There is no workaround.

- CSCuc91056

  Symptom: sip-notify is not getting negotiated in the mid-call. After the midcall invite, rtp-nte to sip-notify dtmf negotiation falls to rtp-nte to default inband-voice

  Conditions: This symptom is observed with IOS version: 15.3(1.2)T.

  Workaround: There is no workaround.

- CSCuc91409

  Symptom: CallManager intermittently fails to reply to SIP messaging when a hostname is present in the host field. This will occur when CallManager fails to resolve the hostname quickly enough resulting in the messaging being dropped.

  Conditions: This symptom is observed TCP or TLS is used. UDP will not experience this issue.

  Workaround: Do not use a hostname in the host field for SIP messaging.

- CSCuc92086

  Symptom: 2921 crashed twice due to http caching. The crashes happened in about 1 month from each other. At least one of them was triggered by issuing **clear http client cache**. However not every issue of "clear http client cache" causes the crash.

  Conditions: This symptom is obsrved when 912 is running as a gateway.

  Workaround: There is no workaround.

- CSCuc92567

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

  Conditions: Extremely rare race condition.

  Workaround: There is no workaround.

- CSCuc93053

  Symptoms: The WCCP stops working after adding Cisco IOS Zone Based Firewall (ZBF. Message of WCCP packets being redirected can be seen but not leaving the Cisco ASR router.

  Conditions: This symptom is observed when Cisco ASR router with netflow and ZBF is enabled under the same interfaces.

  Workaround: Disable netflow on all the interfaces.

- 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.

- 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.

- CSCuc97316

  Symptom: Incorrect **show running-config all** after running **no vxml audioerror.**

  Conditions: This symptom occurs when there is no vxml audioerror in the **show running-config all** command.

  Workaround: Run **show running-config.**

- CSCuc98021

  Symptom: One-way voice audio issue is seen over CUBE after session re-INVITE is sent.

  Conditions: This symptom is observed with the following call flows:

  - Signaling: Cisco IP phone ==> CUCM ==> CUBE ==> CCIPL ==> CCIPL IP phone
  - Media: Cisco IP phone <=== sRTP ==> CUBE <== RTP ==> CCIPL IP phone

  Workaround: Do not use SRTP on the CUCM <-> CUBE leg.

- 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.

- CSCuc98855

  Symptom: For some reason the EzVPN server send the savepwd off. When it does, the client fails to establish the connection.

Conditions: There is no known conditions.

Workaround: Run the client in interactive mode authentication.

- CSCud01502

  Symptom: A crash occurs in CME while accessing a stream in sipSPIDtmfRelaySipNotifyConfigd.

  Conditions: This symptom occurs in CME.

  Workaround: There is no workaround.

- CSCud01905

  Symptom: Match not APN is not working.

  Conditions: This symptom occurs during the basic GTP message flow.

  Workaround: There is no workaround.

- CSCud02357

  Symptoms: The extension mobility feature is failing.

  Conditions: This symptom is observed in Cisco IOS Release 15.3(2)T.

  Workaround: There is no workaround.

- CSCud04066

  Symptom: CPP CVLA traceback appears.

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

  Workaround: There is no workaround.

- CSCud05194

  Symptom: Traceback is seen in 302 consume SDP pass through scenario.

  Conditions: This symptom occurs when the UUT is failing on 15.3(0.19)S.

  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.

- CSCud06171

  Symptom: The Cisco router crashes upon clearing of the AppNav counters.

  Conditions: This symptom can occur in a normal running device.

  Workaround: There is no workaround.

- CSCud06852

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

  Conditions: RP Switchover .

  Workaround: SPA Soft OIR.

- 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.

- CSCud10343

  Symptom: The VG224 phone can not hear FAC tone.

  Conditions: This symptom is observed during the config **cptone br** under voice-port.

  Workaround: Change cptone to us.

- CSCud11761

  Symptom: The **cpp_svr** crashes.

  Conditions: This symptom is obsrved with **Policy-Aggregator** scalability config.

  Workaround: There is no workaround

- CSCud12022

  Symptom: The SPA buffer oversubscription causes a message to be logged indicating the packet drops in the SPA.

  Conditions: This symptom is observed during reconfiguration, flow-control cannot be set correctly on the ESP resulting in broken flow-control on the interface being reconfigured.

  Workaround: There is no workaround.

- 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.

- CSCud11761

  Symptom: The **cpp_svr** crashes.

  Conditions: This symptom is obsrved with **Policy-Aggregator** scalability config.

  Workaround: There is no workaround.

- CSCud14601

  Symptom: iDivert call to voicemail failed in flow-around mode for both consult and blind transfer scenarios

  Conditions: This symptom is observed when running with IOS version 15.3(1.4)T.

Workaround: There is no workaround.

- CSCud16127

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

  Conditions: This symptom is observed when the IMSI is invalid.

  Workaround: There is no workaround.

- CSCud16274

  Symptom:CPP crash with core dump file and traceback.

  Conditions: This symptom is observed when the session setup rate is 10.

  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.

- CSCud19265

  Symptom: CPP error and traceback when ATM PVC sub-interface deleted or reconfigured.

  Conditions: This symptom is observed when ATM PVC in sub-interface is configured under ATM PVP.

  Workaround: There is no workaround.

- CSCud21267

  Symptom: Accesses to the midplane EERPOM or power supply fails.

  Conditions: This symptom is observed when the system has dual RPs.

  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.

- CSCud23420

  Symptom: This is a backout of the PI commit of CSCuc10263.

  Conditions: The initial implementation of enabling logging to CC required dependency on the PI code committed. But after the code review for the PD the PI commit is not required. Hence Backing out.

  Workaround: There is no workaround

- CSCud24079

  Symptom: CUBE could not handle multiple 18x responses with different to-tags in early dialog.

  Conditions: When 18x responses doesn't contain SIP Contact header.

  Workaround: Include Contact header in 18x responses.

- CSCud24321

Symptom: The interface hierarchy gets corrupted during OIR such that subsequent reconfiguration events lead to a system crash. Impacted Platforms: ESP-100 and VXE-2, aka Yoda platforms. Not Impacted Platforms: All CPP10 platforms, i.e. ESP-10, ESP-20, ESP-40, etc. It also does not impact Overlord and ultra.

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

Workaround: Remove FRF.12 before OIR and re-apply it after OIR. While this should work when done manually or via a script, it may be unreliable in the real world where OIR could occur due to swapping out one SPA for another unless the user remembers to disable FRF.12 before swapping the SPAs.

- CSCud24483

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

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

  Workaround: There is no workaround.

- 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.

- CSCud31542

  Symptom: DHCP reply message was dropped in the data plane after RPSO or **clear ipv6 neighbor.**

  Conditions: This symptom is observed during the following situations:

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

  Workaround: The following are the workarounds:

  - Send downstream traffic to the client that will re-learn the neighbor.
  - Clear IPv6 route X::X/prefix <dhcp installing route> to re-learn the neighbor.
  - Client is reconnected after the timeout of DHCP session.
  - Client sends RS or NS.

- CSCud34131

  Symptom: ERSPAN only could monitor ZBFW interface Rx packets.

Conditions: ERSPAN packets will be drop if the ERSPAN output interface is not in same zone with moitor interface

Workaround: Configure ERSPAN output interface with same zone with monitored interface

- CSCud34647

  Symptom: ucode along with the fman_fp cores is seen in the supporting FP80 router.

  Conditions: This symptom is observed on the flapping member link interface in the UUT.

  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.

- 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.

- CSCud36089

  Symptom: **sh per-call buffer list** output shows an extra '**I**' in the LAST UPDATED column.

  Conditions: This symptom is observed when the Per-Call debugging is enabled

  Workaround: There is no workaround.

- CSCud37568

  Symptom: Memory leak in GTP PDP pool.

  Conditions: GTP AIC must be configured.

  Workaround: There is no workaround.

- CSCud37921

  Symptom: Communication broken. 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.

- CSCud38010

  Symptom: Due to the change of CSCud35735: ASR1K: ucode crash @gtp_aic_match_policy. It is a defense for smtp aic, as the function call re_multi_match_ascii may result crash?

  Conditions: When the function re_multi_match_ascii meet some invalid array address,it would return 0xFFFFFFFF as the match length,here in smtp aic,it should be protected from this exception?

  Workaround: There is no workaround.

- CSCud38558

  Symptom: The two causes are:

  – Might be no monitoring.

  - Trackback message appears in log: **1#7e4ed294e9cee774e6d357fbecf1228d errmsg:CB20000 2230 cpp_common_os:D1AD000 BBB0 cpp_common_os:D1AD000 B9C0 cpp_common_os:D1AD000 1903C cpp_fnf_svr_lib:FE68000 15D64 cpp_fnf_svr_lib:FE68000 1C2D0 cpp_fnf_svr_lib:FE68000 18E84 cpp_common_os:D1AD000 10A94 cpp_common_os:D1AD000 110CC evlib:CEF1000 E0DC evlib:CEF1000 104C4 cpp_common_os:D1AD000 127E8:10000000 4710 c:A526000 1E938 c:A526000 1EAE0.**

  Conditions: The issue occurs:

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

  Workaround: Reapply the configuration.

  Workaround: There is no workaround needed here as this is the data used for the information about the peer for the user. No impact.

- CSCud39324

  Symptom: ESP reload

  Conditions: ASCII ALG traffic requiring TCP seq/delta fixup on payload length change due to address translation. This reload could occur rarely with very long lived TCP connections. Workaround: Turn off the ALG likely causing the issue.

- CSCud40015

  Symptom: Client/Server IPs are interchanged in CLI **sh serv-in statis conn** on Peer AC's.

  Conditions: Client/Server IPs are interchanged in CLI **sh serv-in statis conn** on Peer AC's. This symptom is observed when there are 4 AC's in the ACG and the context is up and Operational. Some traffic is sent and only one AC owns that flow. When the CLI **sh service-inse statis conn** is executed on the AC, which owns the flow it shows the right output. But when the same command is executed on other AC's the Client and Server IP 's are interchanged.

  Workaround: There is no workaround.

- CSCud40063

  Symptom: Stale PVP object seen.

  Conditions: Do a RP switchover with a PVP configured on ATM port and cdvt global config enabled on Barbarian SPA.

  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.

- CSCud41501

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

  Conditions: This symptom occurs during the following situations:

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

  - Under the interface config mode, configure the above defined monitor using **[ip | ipv6 | mpls] flow monitor <name> (sampler) [input | output]**
  - Issue the following show command to see the cached records: **show flow monitor <name> cache**.
  - In the output of the above show command, the values displayed for the first and last timestamp fields can be incorrect.

  Workaround: There is no workaround.

- CSCud42197

  Symptom: map-request is missing in xTR.

  Conditions: This symptom is observed in the CLI **lig self all.**

  Workaround: There is no workaround.

- CSCud42595

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

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

  Workaround: There is no workaround.

- CSCud42919

  Symptom: FP crash.

  Conditions: up to 70~80K translation sessions, SIPand H323 mixed traffic

  Workaround: There is no workaround.

- CSCud43620

  Symptoms: The Gateway fails to send ACK after 200 OK while testing DNS/SRV Lookup on a VOIP peer with weight/priority.

  Conditions: This symptom is observed when a Cisco router is loaded with c2900-universalk9-mz.SSA.153-1.7.T image.

  Workaround: There is no workaround.

- CSCud44854

  Symptom: hash table not memset for ALG during intialization.

  Conditions: This symptom occurs during the following conditions:

  - Start sip/h323/... traffic
  - Establish NAT session over 60~70K
  - Send CLI combinations with below actions:
  - clear **ip nat trans ***
  - shutdown inside / outside traffic interfaces
  - remove **nat/alg** config

- reconfig **nat/alg** and unshut interfaces

Workaround: There is no workaround.

- CSCud45750

  Symptom: Extended data forwarding outage when MLPPPoLNS session forwarded to a new link due to a OSPF link change. Possible MLPPP member link session flap.

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

  Workaround: There is no workaround. Also keep in mind that even with the fix associated with bug report, per packet load balancing is NOT supported with MLPPP. Only per destination packet load balancing.

- CSCud47046

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

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

  The following are the different Call scenarios:

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

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

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

  Later call modification makes four calls hair pined together

  Workaround: There is no workaround.

- CSCud49494

  Symptom:ESP crashed 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.

- CSCud49777

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

  Conditions: Perform clear crypto session on the headend. Sessions will be triggered again from SVTI. For few of the sessions, framed route is not installed.

  Workaround: There is no workaround.

- 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.

- CSCud55724

  Symptom: **na-src-adj** table does not work for text userid.

  Conditions: This symptom is seen always.

  Workaround: There is no workaround.

- CSCud56064

  Symptom: iDivert call to voice mail failed after call forward

  Conditions: When running with IOS version - 15.3(1.8)T

  Workaround: There is no workaround.

- CSCud56400

  Symptom: Build breakage occurs due to CSCub81489 partial export to mcp_dec.

  Conditions: This symptom is observed with export to mcp_dec.

  Workaround: There is no workaround.

- CSCud58038

  Symptom: ucode crash is seen with nat tgn mode and CLI operation during traffic

  Conditions: This issue occurs during the conditions:

  - setup sip/h323 traffic
  - shut ->clear ip nat tr * -> unshut
  - remove ip nat shut clear ip nat tr *

  Workaround: There is no workaround.

- CSCud60014

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

  Conditions: This issue occurs during the reconfigurations such as adding a hierarchical policy to an ATM, changing a class-of-service for an ATM VC, etc. and results in a new scheduling hierarchy.

  Workaround: There is no workaround.

- CSCud61316

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

  Conditions: The issue occurs during the following conditions:

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

  Workaround: Manually clear the affected NAT session.

- CSCud61366

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

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

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

- CSCud63126

  Symptom: The crashinfo file is not generated.

  Conditions: This issue is specific to the ASR1K and the RP1. RP2 doesn't have this issue. It has been seen for Software Forced Crashes.

  Workaround: There is no workaround.

- CSCud66316

  Symptom: The log messages for REJECT Create Session Response message is not printed in the sys-log.

  Conditions: This symptom is observed when the GTP AIC is configured in the UUT.

  Workaround: There is no workaround.

- CSCud66955

  Symptom: SPA-2CHT3-CE-ATM is flapping with Nortel Passport due to the fast bouncing of up or down 10s, after the interface is brought up.

  Conditions: This symptom is observed in E3 and DS3 mode.

  Workaround: There is no workaround.

- CSCud70243

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

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

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

- CSCud71253

  Symptom: Outbound traffic does not flow.

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

  Workaround: There is no workaround.

- CSCud72509

  Symptom: The ESP100 is crashed.

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

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

- CSCud72816

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

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

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

- CSCud73594

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

  Conditions: This symptom is observed during the massive sequence of policy attach or detach operations.

  Workaround: There is no workaround.

- CSCud73599

  Symptom: Records are not generated even after several configurations.

  Conditions: This symptom is observed during Config replace or any other massive performance policy configuration.

  Workaround: There is no workaround.

- CSCud73600

  Symptom: The FP is crashed.

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

  Workaround: There is no workaround.

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

- CSCud73652

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

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

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

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

  Workaround: There is no workaround

- CSCud75024

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

  Conditions: The issue occurs during the session teardown.

  Workaround: There is no workaround.

- CSCud75692

  Symptom: Tunnel QoS is broken.

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

Workaround: There is no workaround.

- 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 the packets, presumably, because feature chain is executed.

  Workaround: Disabling MLRE through the configuration command **platform multicast lre off** can be done if condition occurs.

- CSCud77549

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

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

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

- CSCud78649

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

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

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

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

- CSCud79391

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

  Conditions: When loading an **advipservices** image, AVC functionality could not be configured.

  Workaround: There is no workaround.

- CSCud80832

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

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

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

- CSCud81011

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

  Conditions: This symptom is observed only with certain configurations

  Workaround: There is no workaround.

- CSCud86039

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

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

Workaround: There is no workaround.

- CSCud86240

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

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

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

- CSCud88366

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

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

  Workaround: There is no workaround.

- CSCud90021

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

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

  Workaround: There is no workaround.

- CSCud90142

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

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

  Workaround: There is no workaround

- CSCud91102

  Symptom: Router reload.

  Conditions: The issue occurs during the heavy AVC traffics.

  Workaround: There is no workaround.

- CSCud91877

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

  Conditions: The issue occurs always.

  Workaround: There is no workaround

- CSCud91920

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

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

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

- 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.

- CSCud92837

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

  Conditions: The issue occurs when PfR is enabled.

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

- CSCud92879

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

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

  Workaround: There is no workaround.

- CSCue00726

  Symptom: There is no functional impact to the system performance, warning messages will be seen only during initialization of the router and there are no security concerns on these units: ***Dec 16 17:58:02.432: IOSXE_PLATFORM-3-WDC_INVALID_LENGTH WDC length can not be determined: 65535 . *Dec 16 17:58:10.703: PLATFORM_SCC-1-AUTHENTICATION_FAIL Chassis authentication failed *Dec 16 17:58:10.703: IOSXE_AUTHENTICATE-2-AUTHENTICATE_FAILED.** The platform authentication failed.

  Conditions: Programming of Quack & WDC (Watch Dog Certificate) was accidently disabled in manufacturing during the regression testing. This caused units to ship without Quack & WDC programming. These messages show up at boot up for these specific units that had the quack disabled

  Workaround: There is no workaround.

- CSCue05798

  Symptom: Need to backout due to the hardware limitation.

  Conditions: Fix not needed due to the hardware limitation.

  Workaround: There is no workaround.

- CSCue12387

  Symptom: FDT charts in CM GUI are improper.

  Conditions: This symptom is observed due to the inconsistency between actual output of show policy-map target service-context command and its XML equivalent.

  Workaround: Check the corresponding WAAS (WAE) TCP graphs for achieved optimization.

- CSCue14379

Symptom: If a new ATM PVP shaper is configured during the runtime and then a ATM VC with that VPI value is configured, tracebacks will be generated. Router operation will continue but QoS configuration for the VC and VP will be incorrect.

Conditions: A new PVP must be configured and a new VC is configured with that VPI.

Workaround: Configure the new PVP shapers, save the configuration, reboot the router. After the router is rebooted, VCs configured in the shaped VPs will have the correct QoS configuration.

- CSCue15619

  Symptom: SBC CLI hung.

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

  Workaround: There is no workaround.

- CSCue17371

  Symptom: NTE cannot pass through.

  Conditions: The issue occurs for a transcoding call.

  Workaround: There is no workaround.

- CSCue17800

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

  Conditions: Perform 6RD and MPLSoGRE tunnel decapsulation.

  Workaround: There is no workaround.

- CSCue19598

  Symptom: Show service-insertion statistics service-node-group command produces incomplete or incorrect output when multiple SNGs are configured under the service-context.

  Conditions: Multiple SNGs are configured under the service-context

  Workaround: There is no workaround.

- CSCue20394

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

  Conditions: This symptom is observed during an ongoing transmission.

  Workaround: There is no workaround.

- CSCue22084

  Symptom: The Create Session Response message is dropped.

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

  Workaround: There is no workaround.

- CSCue25321

  Symptom: BFD flaps continuously upon ESP switchover.

  Conditions: This symptom is observed during the ESP switchover.

  Workaround: There is no workaround.

- CSCue32352

Symptom: Non-HDLC traffic (Non standard, but customer defined traffic) coming through HDLC interface gets 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.

- CSCue34315

  Symptom: TDL incompatibility

  Conditions: This symptom is seen with the ISSU.

  Workaround: There is no workaround.

- CSCue34591

  Symptom: No Symptoms as such. PTP will come up as a process on both IOS and BINOS.

  Conditions: This symptom is seen when the router is upgraded to XE39 image.

  Workaround: There is no workaround, the PTP process comes up on IOS and BINOS.

- CSCue39090

  Symptom: A very small FM memory leak is observed.

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

  Workaround: There is no workaround.

- CSCue44303

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

  Conditions: This symptom is seen under low memory conditions.

  Workaround: There is no workaround.

- CSCue44651

  Symptom: On ASR1K, with GTP ZBFW pinholes are opened on GTP-U on 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.

- CSCue46537

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

Conditions: This symtom is observed only on ASR1K.

Workaround: Reboot the router.

- CSCue46852

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

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

  Workaround: There is no workaround.

- CSCue51967

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

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

  Workaround: There is no workaround.

- CSCue63181

  Symptom: The Delete PDP Context Response message is dropped.

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

  Workaround: There is no workaround.

- CSCue69075

  Symptom: BDI interface stops forwarding the traffic.

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

  Workaround: Recreate the BDI interface.

- CSCue71410

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

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

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

- CSCue72210

  Symptom: Ping fails when NAT64, PAT, and ZBFW are configured.

  Conditions: Valid zone-pair is configured & ZBFW sessions exists, IPv6 ping fails from pagent. This happens only with NAT64, PAT, and ZBFW combination.

  Workaround: There is no workaround.