



Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.6S

This chapter provides information about the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.6S.



Note

For information about the caveats pertaining to earlier releases, see [Cisco IOS XE 3S Release Notes](#).

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

This chapter contains the following section:

- [Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.6S, page 1226](#)

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.6S

This section contains the following topic:

- [Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.6.1S, page 1227](#)
- [Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.6.1S, page 1228](#)
- [Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.6S, page 1233](#)
- [Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.6.2S, page 1241](#)

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.6.1S

- CSCtu95951

Symptom: The router crashes when scale sessions are cleared or closed when some other actions, such as service-apply, unapply, and timeouts, occur simultaneously.

Conditions: This issue is observed when multiple actions and session-clear occur simultaneously in a scale scenario.

Workaround: Avoid clearing sessions when multiple actions such as the ones specified above are taking place.
- CSCtx44508

Symptom: During initial bulk synchronization, a peer on which IBGP nonstop routing (NSR) is enabled takes a long time to synchronize. Depending on the scale of the setup and the number of routes and paths received from the IBGP peer, synchronization could take up to a few minutes.

Conditions: This issue is observed when NSR is configured for an IBGP peer and the standby route processor (RP) comes up in an asymmetric startup scenario, triggering bulk synchronization.

Workaround: There is no workaround.
- CSCty10285

Symptom: The Web Cache Communication Protocol (WCCP) redirections do not take place on a router that is running Cisco IOS XE Release 3.5S.

Conditions: This issue is observed when Group Encrypted Transport (GET) VPN is configured on a router on which Cisco ASR1000-RP1 is installed.

Workaround: There is no workaround.
- CSCtz37863

Symptom: If IP Control Protocol (IPCP) negotiation fails, an interim update is not sent.

Conditions: This issue is observed when the IPCP configuration is in the dual-stack and IP-saving mode.

Workaround: There is no workaround.
- CSCtz71804

Symptom: A drop in performance is observed when the Dynamic Multipoint Virtual Private Network (DMVPN) is configured with BGP, OSPF, or EIGRP for specific packet sizes.

Conditions: This issue is observed when the DMVPN is configured with Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), or Enhanced Interior Gateway Routing Protocol (EIGRP) for specific packet sizes.

Workaround: There is no workaround.
- CSCtz80342

Symptom: A drop in performance is observed on multicast VPN (mVPN) configured on Cisco ASR1000-RP1 and Cisco ASR1000-ESP10 when the packet size is 1500 bytes or more.

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

Workaround: There is no workaround.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.6.1S

- CSCts40043

Symptoms: The router may ungracefully restart due to a segmentation fault.

Conditions: This issue is observed while modifying the fail-close access control list (ACL) when the same Group Domain of Interpretation crypto map (GDOI CM) is applied to two interfaces and the registration is in the fail-close state in the GETVPN configuration.

Workaround: Remove the crypto map from the interface before modifying the ACL.

- CSCtw46061

Symptom: The IPsec status shows irremovable IPsec sessions. Use the **show crypto eli** command to view the IPsec status.

Conditions: This issue is observed when the router keeps flapping a large number of IPsec sessions.

Workaround: There is no workaround.

- CSCtw78451

Symptoms: The router may reload automatically when multiple users run **show** commands simultaneously.

Conditions: This issue is observed when the router is used as a DMVPN headend router and there are hundreds of tunnels flapping at the same time. It is a timing-related issue that occurs only when there is instability in a large-scale environment.

Workaround: There is no workaround.

- CSCtw87716

Symptom: XML code is displayed in the output of the **show platform hardware qfp {active | standby} system state** command.

Conditions: This issue is observed when the **show platform hardware qfp {active | standby} system state** command is run.

Workaround: There is no workaround. Note that this issue has no impact on the functionality of the router.

- CSCtx15650

Symptom: The Cisco Performance Routing (PfR) dynamic route map is not downloaded to the FMAN-RP process and the FMAN-FP process.

Conditions: This issue is observed when the Cisco PfR feature is used under scale conditions.

Workaround: There is no workaround.

- CSCtx49073

Symptoms: The free space check fails, and the core dump process is not completed.

Conditions: This issue is observed when there is insufficient storage space for the core dump.

Workaround: Ensure that there is enough storage space for the core dump.

- CSCtx77643

Symptom: The embedded services processor crashes and then reloads automatically.

Conditions: This issue is observed when a tunnel interface is configured with a policy map that has only a class default configured on it. The crash may occur under conditions that cause the tunnel to move from one Gigabit Ethernet interface to another.

Workaround: There is no workaround.

- CSCtx81689

Symptom: The router fails to establish Protocol Independent Multicast (PIM) neighbors when IPv6 MVPN is configured.

Conditions: This issue is observed on routers on which Cisco ASR 1000-ESP40 is installed.

Workaround: Disable the Multicast Long-Reach Ethernet feature by running the **platform multicast lre off** command.

- CSCtx84948

Symptoms: The router stops working correctly after consecutive crashes of the embedded services processor. The interfaces are in the Up/Up state, but they do not send traffic.

Conditions: This issue is observed on a router that has redundant embedded services processors.

Workaround: Shut down and restart the disabled interface.

- CSCtx94393

Symptom: The embedded services processor crashes.

Conditions: The symptom is observed under the following conditions:

- Scaled IKEv2 4k IPsec sessions with the FlexVPN dVTI server.
- Scaled IKEv1 1k IPsec sessions with the dVTI server.
- CAC (50) enabled on both the server and the clients.
- DPD (60/15/on-demand) enabled.
- Crypto sessions are cleared from the server every 20 minutes using the **clear crypto session** command.
- Presence of 20 M bidirectional traffic.

Workaround: There is no workaround.

- CSCty02385

Symptom: A drop in traffic is observed when EoMPLS VLAN interworking is configured.

Conditions: This issue is observed only when a VLAN rewrite takes place.

Workaround: Ensure that the same VLAN ID is used on both the PE-facing end and the CE-facing end.

- CSCty19713

Symptom: The embedded services processor crashes.

Conditions: This issue is observed in the NAT Application Layer Gateway for DNS packets.

Workaround:

Disable the DNS Application Layer Gateway by using the following commands:

- **no ip nat service dns tcp**
- **no ip nat service dns udp**

**Note**

After the DNS Application Layer Gateway is disabled, the embedded IP addresses in the DNS packets will not be translated.

- CSCty32548

Symptom: The embedded services processor may reload automatically.

Conditions: This issue may be observed when the CGN mode is in use with a dynamic (that is, not PAT) configuration and you try to run the **clear ip nat trans inside ig il forced** command to clear a dynamic bind that has active child elements.

Workaround: There is no workaround.

- CSCty43302

Symptom: The CPU hog traceback messages may be displayed while the Cisco ASR1000-ESP10 is starting up.

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

Workaround: There is no workaround. Note that the occurrence of this issue does not affect the working of the router.

- CSCty46022

Symptoms: The CPU utilization level of the embedded services processor is constantly high.

Conditions: This issue is observed when the Intelligent Services Gateway (ISG) sessions with a DHCP initiator encounter fragmented traffic whose packet size is small. These packets are punted to the CPU of the embedded services processor.

Workaround: There is no workaround.

- CSCty52047

Symptom: Internet Key Exchange (IKE) security associations (SAs) are not automatically deleted by the Dead Peer Detection (DPD) feature.

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

Workaround: Use the **clear crypto isakmp conn-id** command to manually delete the Internet Security Association and Key Management Protocol (ISAKMP) session that is not responding. The *conn-id* value can be obtained by running the **show crypto isakmp sa** command.

- CSCty54885

Symptoms: The standby RP crashes when the active RP is removed to force a failover.

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

Workaround: Perform a switchover by running the **redundancy forced-switchover** command instead of physically removing the RP.

- CSCty58633

Symptom: The router fails to remove broadband sessions with traffic class features.

To view the Pending-ACK traffic class batch details, use the following commands:

- **show platform software object-manager fp active statistics**
- **show platform software object-manager fp active pending-ack-batch**

Conditions: This issue is observed when the router is subject to high CPU load on embedded services processor, which could be the result of high call per second or RP switch-over.

Workaround: There is no workaround.

- CSCty61212

Symptom: When the GDOI crypto map configured on an interface is removed, the router stops responding.

Conditions: This issue is observed when the GDOI crypto map configured on an interface is removed.

Workaround: There is no workaround.

- CSCty62559

Symptoms: The embedded services processor may crash while a SPA is being reloaded after a RP switchover.

Conditions: This issue is observed when there are approximately 8000 xconnects.

Workaround: There is no workaround.

- CSCty62887

Symptoms: When more than 1024 DTL requests are processed by the SIP ALG, the router may crash.

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

Workaround: There is no workaround.

- CSCty63356

Symptom: A memory leak is observed on the embedded services processor.

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

- Scaled 1000 IKE, 1 Vrf, 4 IPSec, and a total of 4K IPSec sessions
- Multi-SA enabled
- CAC is 50
- DPD is 60/15/periodic
- CES (Cisco 7200 platform) is reloaded approximately every 20 minutes
- Presence of approximately 60 M bidirectional traffic

Workaround: There is no workaround.

- CSCty68402

Symptom: The dropped packet counter fails. In the **show policy-map interface** command output, the Account QoS statistics field displays a value 0 and the same field is displayed multiple times.

Conditions: This condition is observed with the following policy-map interface configuration:

```
policy-map sub-interface-account
class prec1
  police cir 4000000 conform-action transmit exceed-action drop
  account
class prec2
  police cir 3500000 conform-action transmit exceed-action drop
  account
class prec3
  account
class class-default fragment prec4
```

```

    bandwidth remaining ratio 1
    account
policy-map main-interface
  class prec1
    priority level 1
    queue-limit 86 packets
  class prec2
    priority level 2
    queue-limit 78 packets
  class prec3
    bandwidth remaining ratio 1
    random-detect
    queue-limit 70 packets
    class prec4 service-fragment prec4
    shape average 200000
    bandwidth remaining ratio 1
    queue-limit 62 packets
  class class-default
    queue-limit 80 packets

```

Workaround: There is no workaround.

- CSCty69631

Symptom: Multicast forwarding fails due to RPF failures.

Conditions: This issue is observed when the multicast traffic flows through the GRE interface.

Workaround: Reload the router.

- CSCty91888

Symptom: The standby database may not synchronize correctly.

Conditions: This issue is observed when running the Carrier-grade NAT (CGN) feature and the traffic reaches a high setup or teardown rates.

Workaround: There is no workaround.

- CSCtz00728

Symptom: The downstream latency for MLPPPoE traffic and MLPPPoLNS traffic is higher than expected due to an internal queuing delay.

Conditions: This issue is observed with MLPPPoE traffic and MLPPPoLNS traffic.

Workaround: There is no workaround.

- CSCtz01063

Symptom: The embedded services processor crashes if a transcoding call made using the Cisco Unified Border Element (Enterprise Edition) is released immediately after the call is answered.

Conditions: This issue is observed if the transcoding call is released immediately after it is answered.

Workaround: There is no workaround.

- CSCtz13468

Symptom: Auto-RP fails on the POS and ATM interfaces.

Conditions: This issue is observed when the POS SPA or ATM SPA is used with the Auto-RP enabled.

Workaround: There is no workaround.

- CSCtz23514

Symptom: The FMAN-FP process crashes due to memory corruption.

Conditions: This issue is observed when a large number of BBA sessions are opened and closed and the Lawful Intercept feature is enabled on some of these sessions.

Workaround: There is no workaround.

- CSCtz23638

Symptom: The following error message is displayed on the console:

```
PLIM driver informational error txnpTooLittleData
```

Condition: This issue is observed when Cisco ASR 1000-SIP40 is installed on the router.

Workaround: There is no workaround.

- CSCtz44330

Symptom: The following error message is displayed in the syslog:

Uncontrolled due to Exit Mismatch

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

- PfR is enabled on a scale setup using DMVPN as external interface to a large number of remote sites.
- Cisco ASR 1000 is configured as border router.
- All the traffic classes are application prefixes that are controlled using PBR.

Workaround: There is no workaround.

- CSCtz69986

Symptom: The amount of free memory on the router decreases slowly over time. The rate of decrease is approximately 7 MB a day.

Conditions: This issue is observed when the Web Cache Communication Protocol (WCCP) is configured on the interfaces.

Workaround: There is no workaround.

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.6S

This section documents the unexpected behavior that might be seen in Cisco ASR 1000 Series Aggregation Services Routers Release 3.6S.

- CSCtr63443

Symptom: The multicast forwarding plane entry and control plane entry are not consistent with each other.

Conditions: This issue is observed when the BGP local peering interface is changed while active traffic is flowing on the default MDT and data MDT.

Workaround: Clear the forwarding plane entry.

- CSCtr73680

Symptom: The multicast data plane forwarding entry is incomplete. This may result in data getting dropped.

Conditions: This issue is observed under stress testing conditions when BGP sessions and multicast routes are cleared multiple times while running MVPNv6.

Workaround: There is no workaround.

- CSCtt65336

Symptom: When the primary path fails, a degradation of approximately 10 percent is observed in the time that it takes for the traffic to converge to an alternative path.

Conditions: This issue is observed when the router is processing multicast traffic and there are more than 1000 multicast routes.

Workaround: There is no workaround.

- CSCtt94440

Symptom: The route processor may reload automatically.

Conditions: This symptom is observed when the etoken is in use and the **show crypto eli all** command is run.

Workaround: Use the **show crypto eli** command instead of the **show crypto eli all** command.

- CSCtu22167

Symptom: The standby route processor crashes.

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

- Prefixes are unicast through local labels.
- A tunnel is the next hop for these prefixes.

The standby route processor crashes when you modify the topology by, for example, removing or shutting down the physical interface leading to the destination address of the tunnel becoming reachable via the tunnel.

Workaround: Ensure that the tunnel endpoint peer does not advertise the prefixes that must be known to reach the tunnel endpoint.

- CSCtu33110

Symptom: The embedded services processor may crash.

Conditions: This issue is observed when MLPPPoBB is configured and the traffic traversing the subscriber contains fragments that are reassembled into packets larger than 9216 bytes in size.

Workaround: There is no workaround.

- CSCtw47123

Symptom: IPv6 packets that have extension headers are not forwarded on IPsec SVTI tunnels. Instead, they are punted to the CPU. This causes an increase in the CPU utilization level.

Conditions: This issue is observed when IPv6 packets with the hop-by-hop extension header, fragmentation extension header, or authentication extension header are sent over secure IPsec SVTI tunnels.

Workaround: There is no workaround.

- CSCtw59780

Symptom: BGP dynamic neighbor structures at the hub are not cleaned up after the spokes change to the Down state. The output of the **show ip bgp all sum** command continues to display dynamic neighbors.

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

- The scale environment for dynamic neighbors contains several thousand peers.
- The peers are brought up and then removed before they can transition into the Established state.

Workaround: There is no workaround.

- CSCtw61192

Symptom: Routes in EIGRP are in the stuck-in-active condition.

Conditions: This issue is observed when routes in EIGRP are withdrawn. When this happens, the router sends the query to the source of routes originated by the advertising router. The routes then change to the stuck-in-active condition and do not return to the normal condition.

Workaround: There is no workaround.

- CSCtw91913

Symptom: For MPLS interworking on the port channel, if port mode xconnect is configured on one end of the pseudowire and VLAN mode xconnect is configured on the other end, the pseudowire goes down.

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

- Port mode (that is, main interface) xconnect is configured on the port channel.
- The port channel subinterface is configured with the **encap dot1q** command.

Workaround: Remove the port channel subinterface, and then shut down and restart the main interface.

- CSCtw98158

Symptom: When two ATM VPs are configured with cell packing and MCPT timers and connected locally (that is, they are configured for ATM local switching by using the **connect** command), the router may crash while defaulting the ATM interfaces.

Conditions: This issue is observed when cell packing and MCPT timers are configured along with local switching.

Workaround: There is no workaround.

- CSCtw99035

Symptom: The multicast control plane does not repopulate the BGP auto-discovery route.

Conditions: This issue is observed when the **clear bgp ipv6 mvpn *** command is run on an MVPNv6-only configuration (that is, MVPNv4 is not configured).

Workaround: There is no workaround.

- CSCtx05726

Symptom: The standby route processor may crash while configuration information is being copied from a TFTP server.

Conditions: This issue is observed while configuration information is being copied from a TFTP server.

Workaround: There is no workaround. Note that when the standby route processor reboots after the crash, the configurations on the active route processor are correctly synchronized to the standby route processor.

- CSCtx13741

Symptom: The crashinfo file cannot be generated.

Conditions: This issue is observed when the router crashes due to a software issue.

Workaround: There is no workaround.

- CSCtx32935

Symptom: The permanent license automatically changes back to the evaluation license.

Conditions: This issue is observed when the router is reloaded after the installation of the permanent license.

Workaround: There is no workaround.

- CSCtx42223

Symptom: The connection with an FRR client that is registered for a BFD session is lost after an SSO. The FRR client is not notified when the BFD session detects the failure.

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

Workaround: There is no workaround.

- CSCtx44508

Symptom: There is a delay in route processor synchronization after an SSO.

Conditions: This issue is observed when IBGP NSR is enabled, and under scale conditions.

Workaround: There is no workaround.

- CSCtx48753

Symptom: In Release 3.6.0, configurations that contain PPP sessions use more memory when compared with earlier releases.

Conditions: This issue is observed in configurations that contain PPP sessions.

Workaround: There is no workaround.

- CSCtx50202

Symptom: The ERSAN multilink range and description are lost.

Conditions: This issue is observed after a route processor switchover.

Workaround: There is no workaround.

- CSCtx52042

Symptom: The PMIP crashes when IPv6 bindings on a peer router are cleared.

Conditions: This issue is observed on IPv6 mobile nodes.

Workaround: There is no workaround.

- CSCtx53391

Symptom: uCode may crash when the router is reloaded or when interfaces are shut down and restarted.

Conditions: This issue may be observed when more than 200 VC bundles are configured under an interface that also has more than 200 PVCs with IPv6 configured.

Workaround: There is no workaround. Try to avoid configuring VC bundles and PVCs with IPv6 addresses under the same main interface.

- CSCtx60094

Symptom: Type 1 MVPN routes are not created.

Conditions: This issue is observed when the IP address of a loopback interface is changed.

Workaround: Create a dummy neighbor under the **address-family ipv4 mvpn** configuration or the **address-family ipv6 mvpn** configuration. Alternatively, unconfigure and reconfigure the MDT group under the VRF configuration.

- CSCtx64813

Symptom: After the crypto map is deleted, the configuration under the crypto map does not get fully cleaned up. Because this standalone configuration is created by the nonvolatile generation (NVGEN) process, the standby route processor resets automatically due to configuration synchronization failure.

Conditions: Delete the incomplete crypto-map having one of the command **set security-association lifetime kilobytes**.

Workaround: There is no workaround.

- CSCtx75609

Symptom: The AToM virtual circuit does not come up in the standby route processor.

Conditions: This issue is observed when xconnect is configured on the CEM circuit.

Workaround: There is no workaround.

- CSCtx75661

Symptom: The MTU value for a virtual token ring interface changes when a subinterface is created on the virtual token ring interface.

Conditions: This issue is observed after a subinterface is created.

Workaround: There is no workaround.

- CSCtx80446

Symptom: When the **no authentication** command is run on one BFD template, other MHOP BFD sessions on which authentication has been configured may change to the Down state.

Conditions: This issue is observed when there are multiple sessions using different maps and templates.

Workaround: There is no workaround.

- CSCtx87332

Symptom: The **gshut** command either modifies the loc_pref property for all the nets or does not modify the loc_pref property for any net.

Condition: This issue is observed when more than one customer edge router in a VRF belongs to the same autonomous system.

Workaround: There is no workaround.

- CSCtx92716

Symptom: The router crashes when service policies are removed and added on port-mode cell-packed interfaces.

Conditions: This issue is observed when service policies are removed and added on port-mode cell-packed interfaces.

Workaround: There is no workaround.

- CSCtx96605

Symptom: An ISSU support message is displayed after the router is reloaded.

Conditions: This issue is observed after the router is reloaded.

Workaround: There is no workaround. Note that the occurrence of this issue does not affect the working of the router.

- CSCty02385

Symptom: A drop in traffic is observed when EoMPLS VLAN interworking is configured.

Conditions: This issue is observed only when a VLAN rewrite takes place.

Workaround: Ensure that the same VLAN ID is used on both the PE-facing end and the CE-facing end.

- CSCty09535

Symptom: Some BGP IPv4 packet loss may be observed after an ISSU upgrade from Release 3.5.0 to Release 3.6.0 on a Cisco ASR 1004 Router on which RP2 is installed.

Conditions: This issue is observed after an ISSU upgrade from Release 3.5.0 to Release 3.6.0 on a Cisco ASR 1004 Router on which RP2 is installed.

Workaround: There is no workaround.

- CSCty13699

Symptom: When the L2VPN Pseudowire Stitching feature is configured between a static segment and a dynamic segment, both segments may move to the Down state.

Conditions: This issue is observed when the L2VPN Pseudowire Stitching feature is configured between a static segment and a dynamic segment.

Workaround: There is no workaround.

- CSCty16620

Symptom: The backup pseudowire in SVIEoMPLS does not come up after the router is reloaded.

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

- The remote router on the backup pseudowire does not support the TLV pseudowire status.
- The **no status TLV** command is not run on the pseudowire class used in the pseudowire that does not support the TLV pseudowire status.

Workaround: To avoid this issue, if the remote side does not support the pseudowire TLV status, run the **no status TLV** command on the pseudowire class that is used. If this issue does occur, reprovision the backup pseudowire after the reload operation.

- CSCty24937

Symptom: Ternary content-addressable memory (TCAM) may get exhausted, and the embedded services processor may crash.

Conditions: This issue is observed when more than 300 class maps, each matching 64 security tags, are configured as part of Cisco TrustSec ID Firewall (IDFW) on a Cisco ASR 1002 Router or on any Cisco ASR 1000 Series Aggregation Services Router on which Cisco ASR 1000-RP1 and Cisco ASR 1000-ESP10 are installed.

Workaround: There is no workaround.

- CSCty25773

Symptom: A traceback message may be displayed after a route processor switchover.

Conditions: This issue is observed when MPLS TE configuration is applied over pseudowire configuration.

Workaround: There is no workaround.
- CSCty28813

Symptom: If the default MDT address configured for one VRF is the same as the data MDT address of another VRF, a CPU hog message may be displayed or the router may crash.

Conditions: This issue is observed when the default MDT address configured for one VRF is the same as the data MDT address of another VRF.

Workaround: There is no workaround.
- CSCty29277

Symptom: The Cisco Flexible NetFlow exporter continues to export information about deleted interfaces.

Conditions: This issue is observed when subinterfaces are deleted while an active Cisco Flexible NetFlow exporter is in use.

Workaround: There is no workaround.
- CSCty30886

Symptom: The standby route processor may crash when you try to bring up a PPPoE session.

Conditions: This issue is observed when both the following configurations are set up on the active route processor:

 - An invalid IP address pool is configured under the virtual template.
 - The **aaa authorization network default group radius-server** command is used to configure remote authentication and authorization. However, the local AAA server is used for this purpose under the virtual template.

Workaround: There is no workaround.
- CSCty32548

Symptom: The embedded services processor may reload automatically when the **clear ip nat trans inside ig il forced** command is run to clear a dynamic bind that has active elements.

Conditions: This issue is observed in the CGN mode with a dynamic configuration, that is, not a PAT configuration.

Workaround: There is no workaround.
- CSCty35391

Symptom: The router may take a long time to boot and to complete bulk configuration synchronization.

Conditions: This issue is observed when a large number of VPLS VCs and EVCs are configured.

Workaround: There is no workaround.
- CSCty43302

Symptom: CPU hog traceback messages may be displayed while the Cisco ASR1000-ESP10 is starting up.

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

Workaround: There is no workaround. Note that the occurrence of this issue does not affect the working of the router.

- CSCty46058

Symptom: Shutting down a static multisegment VFI causes traffic to flow in one direction.

Conditions: This issue is observed when you configure a point-to-point VFI with two static neighbors and then shut down the VFI by using the **shutdown** command.

Workaround: There is no workaround.

- CSCty52524

Symptom: Traffic may fail when a route map is configured on an IPv6 interface.

Conditions: This issue is observed when a route map is configured on an IPv6 interface.

Workaround: There is no workaround.

- CSCty54187

Symptom: The following error message is displayed:

%IPSEC-3-RECVD_PKT_NOT_IPSEC:Rec'd packet not an IPSEC packet.

Conditions: This issue is observed when the IKEv2 profile is configured with IVRF.

Workaround: There is no workaround.

- CSCty54702

Symptom: The embedded services processor may crash during a route processor switchover.

Conditions: This issue is observed when ISG DHCP sessions are present during the SNMP lawful intercept process.

Workaround: There is no workaround.

- CSCty55118

Symptom: Pending issues and tracebacks are observed.

Conditions: This issue is observed when a neighbor router reloads.

Workaround: There is no workaround.

- CSCty55408

Symptom: Pending issues and acknowledgments are observed after unconfiguring and then reconfiguring the same scale configuration while traffic is running.

Conditions: This issue is observed after unconfiguring and then reconfiguring the same scale configuration while traffic is running.

Workaround: There is no workaround.

- CSCty78454

Symptom: The configured or default DNS timeout interval in the parameter map is not used for DNS sessions. Instead, the UDP timeout interval is used for the DNS sessions.

Conditions: This issue is observed when a UDP timeout interval is configured for DNS sessions.

Workaround: Configure a new class map to match the DNS traffic that is affected, and then configure a new parameter map for this class map. Ensure that the UDP timeout interval specified in the new parameter map is the same as the required DNS timeout interval.

- CSCto58710

Symptoms: Certificate validation fails when the CRL is not retrieved.

Conditions: This issue is observed when a Cisco ASR 1000 Series Aggregation Services Router attempts to retrieve a CRL using LDAP, and the LDAP server is in a VRF.

Workaround: Use a certificate map to revoke certificates or publish the CRL to an HTTP server and configure CDP override to fetch the CRL.

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.6.2S

- CSCtz77171

Symptoms: Subscriber drops are not reported in mod4 accounting.

Conditions: This symptom is observed on checking policy-map interface for accounting QoS statistics on a port-channel subinterface.

Workaround: There is no workaround.

- CSCtz13465

Symptoms: High CPU is seen on Enhanced FlexWAN module due to interrupts with traffic.

Conditions: This symptom is observed in an interface with a policy installed.

Workaround: There is no workaround.

- CSCua07228

Symptoms: Locally generated traffic is not encrypted when crypto map is applied to LISP interface.

Conditions: GET VPN or static crypto map is configured on LISP interface to encrypt traffic between LISP E-IDs.

Workaround: There is no workaround.

- CSCty41336

Symptoms: Forward-alarm AIS does not work on CESoPSN circuits.

Conditions: This symptom occurs when you create SAToP and CESoPSN circuits and configure **forward-alarm ais**.

Workaround: There is no workaround.

- CSCua26487

Symptoms: SNMP loops at OID 1.3.6.1.4.1.9.9.645.1.2.1.1.1, and as a result, SNMP walk fails.

Conditions: This symptom is observed only on the SNMP getbulk request on 1.3.6.1.4.1.9.9.645.1.2.1.1.1.

Workaround: Exclude the MIB table from SNMP walk using SNMP view. See the following configurations:

```
snmp-server view view name iso included snmp-server view view name ceeSubInterfaceTable excluded snmp-server community community view view name interfaceTable excluded snmp-server community community view view name
```

- CSCtz89485

Symptoms: NAT traffic passes through the new standby router following HSRP switchover.

Conditions: This symptom is observed with HA NAT (NAT with HSRP) mappings with inside global addresses that overlap a subnet owned by a router interface.

Workaround: Each of the following actions must be performed:

- Force a HSRP switchover so that the initial standby router takes activity.
- Remove and re-add HSRP NAT mappings on the newly active router.
- Force a HSRP switchover back to the initially active router.

- CSCua13418

Symptoms: RP-Announce packets are replicated across all the tunnel interfaces and the count of replication is equal to the number of tunnel interfaces.

For example, if there are 3 tunnel interfaces, then each tunnel should forward 1 RP-Announce packet each minute (with the default timer configured). However, in this case, each tunnel is forwarding 3 RP-Announce packets across each tunnel interface. This issue is not specific to the number of interfaces. It can happen with any number of tunnel interfaces.

Conditions: This symptom is observed when filter-autorp is configured with the **ip multicast boundary** command. This issue is also seen on the Cisco 3725 router, where the incoming packets are replicated because of the **filter-autorp** command.

Workaround: Removing **filter-autorp** command resolves the issue. However, you need to remove the **pim** and **boundary** commands first, and then reapply the pim and boundary list without the **filter-autorp** keyword. Also, doing this might lead to redesigning of the topology to meet specific requirements.

To remove the **filter-autorp** command, perform the following configuration:

```
int Tun X
no ip pim sparse-dense mode
no ip multicast boundary XXXXXX filter-autorp
int TuX
ip pim sparse-dense mode
ip multicast boundary XXXXXX
```

- CSCtz82716

Symptoms: ESP crashes on changing the tunnel mode from IPSec v4 to IPSec v6.

Conditions: ESP crashes on changing the tunnel mode from IPSec v4 to IPSec v6 with online traffic

Workaround: Shutdown the tunnel before changing the tunnel mode.

- CSCub08714

Symptoms: Poor performance for multicast on ASR 1000 router over DMVPN.

Conditions: This symptom is observed in the following conditions:

- Multicast packet has to come on a Tunnel interface (not a physical interface).
- NS (negate signaling) flag has to be set on one of the interfaces in the MFIB (S,G) entry.

If both these conditions are met, then the packet is punted to control plane and forwarded in both the software and the hardware, thus causing duplicates. The NS punts are periodic or throttled, and not all multicast packets are punted because of NS. Thus the duplication is intermittent or periodic.

Workaround: There is no workaround.

- CSCua77720

Symptoms: **cpp_svr restart** is seen on Optimized Edge Routing (OER) border on tunnel flap (external interface) or configuration replace.

Conditions: Performance Routing (PfR) external i/f flapping or MC/BR session flapping.

Workaround: There is no workaround.

- CSCub01576

Symptoms: Embedded Services Processor (ESP) reloads on the Cisco ASR 1000 router due to ucode crash.

Conditions: This symptom is observed on the Cisco ASR 1000 router where the Layer 4 Redirect feature is configured. This problem was first introduced in Cisco Release 15.2(01)S. This issue may not be seen in some customer environments to about once-a-week in medium-sized high CPS ISG production networks.

Workaround: There is no workaround.

- CSCua87877

Symptoms: A crash occurs in ucode.

Conditions: This symptom is observed with 160 cps SIP calls.

Workaround: There is no workaround.

- CSCua66308

Symptoms: Classification-related error messages and tracebacks are seen on the CLI console, and the configuration is not downloaded to the data path.

Conditions: This symptom is observed in large configurations with multiple deny statements.

Workaround: Observe caution when using deny statements in a configuration.

- CSCua10815

Symptoms: FP Memory is leaking and after sometime, the memory will crash.

Conditions: If IPSec + WCCP is configured, then due to large number of debug log messages in the cpp_cp_F0-0.log file, there is a memory leak in CPP and FP is crashed.

Workaround: There is no workaround.

- CSCua77466

Symptoms: NBAR does not work after subpackage ISSU on a single RP1, although the CLI shows that NBAR is up.

Conditions: This is a timing issue and may or may not appear depending on configuration and system hardware and so on. This issue seems to happen consistently with the upgrade of 3.5.2S to 3.7S on an ASR 1004 router with RP1.

Workaround: Restart the router after ISSU.

- CSCua79516

Symptoms: SYN packets, which are required to establish FTP-data connections, are sporadically dropped at the Cisco ASR 1000 router.

Conditions: This symptom is observed under the following conditions on ASR 1000 router:

- Using the active mode File Transfer Protocol (FTP).
- Using Port Address Translation (PAT).

Workaround: Each of the following work arounds must be performed:

- Use the passive mode FTP.
- Use the static Network Address Translation (NAT) or dynamic NAT configuration.

- CSCua66250

Symptoms: After Locator Identifier Separation Protocol (LISP) encapsulation, in certain conditions, if the packet size is greater than the path MTU size, then the packets could end up getting fragmented and the inner header may not be copied correctly to all the fragments, causing the packets to be dropped.

Conditions: The LISP Ingress Tunnel Router (ITR) encapsulating a packet is not setting the **Don't Fragment** bit in the outer IP header. Therefore, ICMP Destination Unreachable message with bigger error code datagram is not returned to the encapsulating ITR.

Workaround: Configuring IP MTU less than the path MTU on the LISP0 interface or the egress interface on a LISP ITR causes the packets to be fragmented by the LISP ITR and then LISP encapsulated to the destination.

- CSCua27842

Symptoms: The Cisco ASR 1000 router crashes in firewall code due to NULL l4_info pointer. Day 1 issue.

Conditions: This symptom occurs when the Cisco ASR 1000 router acts as the MPLS L3VPN UHP. It crashes because FW/NAT requires the l4_info to be set. To trigger this issue, the following features must be configured:

- MPLS L3VPN (PE)
- Zone Based FW/NAT
- MPLS and MP-BGP load balance configured towards upstream router.

Workaround: There is no workaround.

- CSCty10285

Symptoms: WCCP redirection does not happen with a Cisco ASR 1000 router running Cisco IOS XE Release 3.5 RP1.

Conditions: This symptom occurs when GetVPN is used.

Workaround: There is no workaround.

- CSCua23997

Symptoms: Continuous ESP crash is seen after dropping packets due to unsupported OCE.

Conditions: This symptom is observed when OCE is unsupported.

Workaround: There is no workaround.

- CSCtu33110

Symptoms: While configuring or running virtual fragmentation reassembly on the virtual template that serves MLPPPoBB calls, the FP crashed in **ip_reass/frag_info.c**.

Conditions: Device configured for virtual fragmentation reassembly on the virtual template that serves MLPPPoBB calls.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement.

This issue will be addressed using normal resolution channels. If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtz26658

Symptoms: The Cisco ASR 1000 router acts as GET VPN GM. Small UDP fragments (21 to 25 bytes, IP header included) coming in through the IPsec are dropped.

Conditions: This symptom occurs when the Cisco ASR 1000 router acts as GET VPN GM and TBAR is enabled for the group.

Workaround: There is no workaround. Disabling TBAR is not recommended as a workaround because of the operational impact of the change on a live GET VPN network.

- CSCtz38558

Symptoms: The traceback may be seen on an ASR 1000 router when processing some IPv6 malformed packets.

Conditions: IPv6 packet is malformed.

Workaround: There is no workaround.

Additional Information: Packet will be dropped.

- CSCtz82711

Symptoms: Datapath session would not open for PDP create.

Conditions: This symptom is observed when SGSN sends echo request before PDP_CREATE_REQ.

Workaround: There is no workaround.

- CSCtz67785

Symptoms: The Cisco ASR 1000 router may experience a Control Plane Policing (CPP) crash.

Conditions: This symptom occurs when the router is configured for Session Border Controller (SBC). During periods of high traffic, FP reports a lot of media up events to RP, which can crash FP.

Workaround: If **ip nbar protocol-discovery** command is enabled, it may exacerbate the crashes. Removing it may provide some stability.

- CSCtz92658

Symptoms: Continuous QMOVESTUCK error messages on console for multilink frame relay (MFR) interface.

Conditions: Either on controller shut/noshut or router reload with MFR configurations.

Workaround: There is no workaround.

- CSCtz38394

Symptoms: FP (cpp_cp_svr anf fman_fp_image) crash.

Conditions: MFR member link delete or add is followed by bundle delete or add.

Workaround: There is no workaround.