Release 2.2 Caveats

Caveats describe unexpected behavior in Cisco IOS XE Release 2. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

This section contains open and resolved caveats for the current Cisco IOS XE maintenance release.

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://www.cisco.com/en/US/docs/internetworking/terms_acronyms/ita.html

This section consists of the following subsections:

Open Caveats—Cisco IOS XE Release 2.2.3

This section documents possible unexpected behavior by Cisco IOS XE Release 2.2.3.

- CSCek77178

  If the **clear ip bgp** *neighbor address* **soft out** command is issued to each Interior Border Gateway Protocol (IBGP) neighbor with a 5 second or greater delay between **clear** commands, the route will be cleared for the first iBGP neighbor but does not clear on the other peers. Subsequent **clear** commands do not clear the remaining routes.

  This condition is observed when a Border Gateway Protocol (BGP) route is advertised to iBGP neighbors residing under the same peer group, and a filter list is applied to deny the route from going out to the iBGP neighbors.

  Workaround: The remaining routes clear if the delay between the **clear** commands is removed.

- CSCsj78195

  The **ip nat inside source static network** command allows route maps to be configured when defining static network translations on a Cisco ASR 1000 Series Router.

  The current implementation of NAT and route maps does not support the use of route maps with a static network translation, therefore the command should not allow this configuration.

- CSCsm98756

  CPU usage peaks at 99 percent for a sustained period when the **show run | inc ipv6 route** command is issued with a large-scale configuration (thousands of VLANs) on a Cisco ASR 1000 Series Router. In addition, various control plane functions such as Session Border Controller (SBC) call setup may not function as expected.

  Workaround: Redirect the **show run** command output to a file for post-processing, or save the running configuration to the startup-configuration on the bootflash and then view the running configuration by executing the s**how configuration** command from the IOS console.

- CSCso09886

  When the **show zone security** and **show zone-pair security** commands are executed on the Cisco ASR 1000 Series Router, the console terminal spews all configured zones and zone-pairs.

  This condition occurs when the number of zones and zone-pairs configured exceeds the terminal length value.

  There are no known workarounds.

- CSCso80547

  After online insertion and removal (OIR) insertion of a SPA on the Cisco ASR 1000 Series Router, the traffic flowing through other SPAs in the SIP are affected/dropped for a few seconds.

  This condition is observed when four POS OC-48 SPAs are used in a single SIP, line-rate traffic is flowing through the SPAs, and one of the OC48 SPAs is OIR removed and inserted into the system.

  There are no known workarounds.

- CSCsq70140

  The following error message appears on the Cisco ASR 1002 Router and the Cisco ASR 1004 Router:

  ```
  No memory available: Update of NVRAM config failed!
  ```

  This message appears more frequently when the user is saving a very big configuration, such as a configuration with 16K interfaces on a Cisco ASR 1002 Router or Cisco ASR 1004 Router. This problem is not seen on the Cisco ASR 1006 Router.

  There are no known workarounds.

- CSCsq73935

  When a 1xCHSTM1/OC3-SPA is configured with Sonet framing/t3 mode an invalid instance of “0” is getting populated for tabular objects in the dsx3ConfigTable.

  Workaround: If the mode is set to “ct3” or “ct3-e1”, the “0” instances are not returned.

- CSCsq76871

  Under certain circumstances, the Cisco ASR 1000 Series Router drops logging messages from the console while the startup configuration is being parsed.

  This condition occurs because under certain configurations the buffered log output differs from the console output. In these configurations, some logging messages are dropped by the console, but are saved within the buffered log.

  Workaround: Increase the size of the synchronous logging queues by configuring a large enough logging synchronous level 0 limit for the console line so that log messages are no longer dropped from the console during configuration boot.

  For example:

  ```
  line con 0
  logging synchronous level 0 limit 5000
  stopbits 1
  ```

- CSCsq77838

  A memory leak can occur in the QuantumFlow Processor (QFP) datapath when the Cisco ASR 1000 Series Router has to reassemble fragmented IP packets over an IP tunnel at very high rates (of the order of 5Gbps or more.) When this condition occurs, the following error message is displayed on on the console:

  ```
  %MEM_MGR-3-MALLOC_NO_MEM: pool handle 0x8db00000, size 144
  ```

  Workaround: Avoid fragmentation on the IP tunnel router header so that the tunnel end point on the router does not need to perform reassembly by configuring the IP Maximum Transmission Unit (MTU) of the tunnel interface to be small enough so that the physical interface level does not need to fragment packets based on the physical interface's IP MTU.

- CSCsq91659

  When a 1xCHSTM-OC3 SPA on the Cisco ASR 1000 Series Router is configured in unframed E1 mode and the SPA is reloaded using the **hw-module** *subslot* **reload** command, dsx1LineStatus returns an invalid value of "0."

  There are no known workarounds.

- CSCsr22866

  Enhanced Interior Gateway Routing Protocol (EIGRP) Peer MIB information is missing from the EigrpPeerTable on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsr50040

  If you disable **aaa policy interface-config allow-subinterface** on the Cisco ASR 1000 Series Router on a subinterface that has RADIUS attributes (such as an lcp:interface-config) creating full virtual access for broadband access (BBA) sessions, the system may report error messages and tracebacks.

  Workaround: Configure **aaa policy interface-config allow-subinterface** locally on the router.

- CSCsr68177

  Disabling and enabling the Cisco Discovery Protocol (CDP) on the Cisco ASR 1000 Series Router causes an interface associated with virtual routing and forwarding (VRF) instances to flap.

  Workaround: Remove VRF configurations from the interface.

- CSCsr81066

  When a Cisco ASR 1000 Series Router is configured with more than 140 PVCs and a packet size above 1490, Frame Relay PVC statistics are not updated properly

  There are no known workarounds.

- CSCsr87974

  When the online insertion and removal (OIR) of a SIP is performed on a Cisco ASR 1000 Series Router, traceback occurs at fibidb_configure_lc_ipfib. No functional impact is observed.

  There are no known workarounds.

- CSCsr90264

  When RADIUS authentication is used and an identical zone statement is downloaded from RADIUS as an existing zone statement in the virtual-template, subscriber call attempts fail. The router logs include the following message:

  ```
  Zoning is currently not configured for interface Virtual-Access
  ```

  Workaround: Ensure that when the **aaa policy interface-config allow-subinterface** statement is configured for the virtual-template, the analogous **lcp:interface-config=allow-subinterface=yes** statement is either not configured by RADIUS or uses a different zone name.

- CSCsr95180

  The **show platform hardware** command output is incorrect for some IPv4 routes on a Cisco ASR 1000 Series Router.

  This condition occurs when IPv4 multicast is configured, the **show platform hardware** command is executed for the multicast prefix, and the prefix has ".0" at the end (for example, 225.3.2.0/32).

  There are no known workarounds.

- CSCsu44557

  On a Cisco ASR 1000 Series Router, the memory allocation for Border Gateway Protocol (BGP) processes on the Route Processor (RP) increases after clearing BGP sessions. In addition, the BGP summary counter is also incorrectly incremented.

  There are no known workarounds.

- CSCsu45138

  On a Cisco ASR 1000 Series Router, the Service Control Engine (SCE) sends the wrong IP address in a session query request to the Intelligent Services Gateway (ISG).

  There are no known workarounds.

- CSCsu59865

  The Route Processor (RP) on a Cisco ASR 1000 Series Router reloads when the Border Gateway Protocol (BGP) process is removed while its neighbors are still active.

  Workaround: Remove the BGP neighbors before removing the BGP process.

- CSCsv38148

  When a Cisco ASR 1000 Series Router that is configured as a Virtual Router Redundancy Protocol (VRRP) master sends a ping to the virtual IP (VIP) address, the IP address in the Internet Control Management Protocol (ICMP) echo reply is set to the source address of the physical interface on the router. The IP address returned will not be the VRRP VIP address. This behavior may affect some monitoring systems that require that a ping to the VIP be answered by the VIP address and not the router's physical address.

  There are no known workarounds.

- CSCsv47212

  Under rare conditions, the Route Processor (RP) on a Cisco ASR 1000 Series Router may reload when the running configuration is saved to NVRAM.

  This condition is observed when the running configuration is written to NVRAM with minor modifications (such as adding or deleting a few VLANs) every 15 minutes for several days in a low memory environment.

  There are no known workarounds.

- CSCsv61458

  On a Cisco ASR 1000 Series Router that is configured as a PE router, changes made by the **mpls ip propagate-ttl** command do not take effect until the **mpls ip** command is deleted and replaced on the interface.

  There are no known workarounds.

- CSCsv66694

  When a Cisco ASR 1000 Series Router and a Cisco 7300 Series Router are enhanced Interior Gateway Routing Protocol (EIGRP) neighbors and the Cisco ASR 1000 Series Router redistributes a static route into EIGRP with a route map and sets a tag (such as 1111), the routing table on the Cisco 7300 Series Router and the EIGRP topology table do not show the as tag being set.

  There are no known workarounds.

- CSCsv79583

  The Cisco Coarse Wavelength-Division Multiplexing (CWDM) Small Form-Factor Pluggable (SFP) does not work on Cisco ASR 1002 4XGE-BUILT-IN ports. The following error text is returned:

```
%TRANSCEIVER-3-NOT_COMPATIBLE: SIP0/0: Detected for transceiver module in
GigabitEthernet0/0/0, module disabled
%TRANSCEIVER-6-REMOVED: SIP0/0: Transceiver module removed from GigabitEthernet0/0/0
%TRANSCEIVER-6-INSERTED: SIP0/1: transceiver module inserted in GigabitEthernet0/1/0
%TRANSCEIVER-3-NOT_COMPATIBLE: SIP0/1: Detected for transceiver module in
GigabitEthernet0/1/0, module disabled
%TRANSCEIVER-6-REMOVED: SIP0/1: Transceiver module removed from GigabitEthernet0/1/0
```

  There are no known workarounds.

- CSCsw15883

  When an attempt is made to scale External BGP (eBGP) with Policy Based Routing (PBR) on a single physical interface with more than 500 sessions in a VRF Lite configuration, the standby Route Processor (RP) resets.

  The condition is observed only with scaled configurations, such as 1K eBGP sessions between the CE and the PE and 500 sessions between the CE and the customer network.

  There are no known workarounds.

- CSCsw33109

  On a Cisco ASR 1000 Series Router, when you apply a Quality of Service (QoS) policy map on a Virtual Template (VT) interface that is used by Multihop to terminate sessions and tunnels received from the L2TP Access Concentrator (LAC), all tunnels and sessions drop.

  Workaround: Do not apply a QoS policy map on a VT interface in Multihop.

- CSCsw38686/CSCsw71222

  In rare conditions, after performing a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router, the new standby RP may fail during the reload process and dump core.

  Although there are no known workarounds, after dumping core, the standby RP will reset and perform normally after it restarts.

- CSCsw46873

  When the Cisco ASR 1000 Series Router is configured as a Multicast router and packets are transmitted intermittently in an interval that is larger than the normal registry timeout period (typically, 3 minutes), the initial packet of a multicast stream may not be transmitted from source to subscribers successfully.

  This condition is observed for both Protocol Independent Multicast - Sparse Mode (PIM-SM) and Protocol Independent Multicast - Dense Mode (PIM-DM) and for both IPv4 and IPv6.

  There are no known workarounds.

- CSCsw69695

  The Cisco ASR 1000 Series Router incorrectly sends Intermediate System-to-Intermediate system IS-IS control packets to the low queue. This behavior may cause IS-IS neighbors to flap during congestion.

  Workaround: Map IS-IS packets to the high queue by configuring a Quality of Service (QoS) priority queue policy to match the well-known IS-IS MAC addresses of 0180.C200.0014 and 0180.C200.0015.

- CSCsw72162

  Border Gateway Protocol (BGP) sessions flap on the Cisco ASR 1000 Series Router when the links between peers are load balanced and have different maximum transmission unit (MTU) values. Under certain scenarios, this configuration results in the fragmentation of BGP protocol packets, which can cause drops of these packet.

  Workaround: By default, Path MTU (PMTU) discovery is enabled for BGP. To avoid this problem, disable PMTU discovery by using the following command:

  neighbor *x.x.x.x* **transport path-mtu-discovery disable**

- CSCsw75587

  When a CT3/DS0 SPA is installed on a Cisco ASR 1000 Series Router that is connected back-to-back with an MC-2T3+ PA on a Cisco 7200 Series Router, the interface may go down if the Cisco ASR 1000 Series Router reloads.

  Workaround: Perform a soft online insertion and removal (OIR) of the MC-2T3+ PA on the Cisco 7200 Series Router to bring the interface back up.

- CSCsx04070

  The Cisco ASR 1000 Series Router is not correctly handling double encryption with IPSec IPv4 tunnel mode.

  This condition is observed under the following configuration scenario:

  rtr_A ------ ASR1 ------ ASR2 ---- rtr_B

  where:

  - There is a transit IPSec tunnel between device A and B.
  - There is an IPSec static virtual tunnel interface (sVTI) between ASR1 and ASR2 that is supposed to encrypt the transit IPSec packets again.

  The tunnel between rtr_A and rtr_B gets established correctly, but encrypted traffic cannot be sent over the already encrypted tunnel between the routers because of double Encapsulating Security Payload (ESP) headers.

Note that when Generic Routing Encapsulation (GRE) mode is used on the tunnel, encrypted traffic can be sent because there is a GRE header between the ESP headers.

Workaround: Use GRE mode on the tunnel instead of IPSec IPv4 tunnel mode.

- CSCsx13442

  After executing the **shut/no shut** commands on a hub tunnel interface on a Cisco ASR 1000 Series Router, the spoke cannot restore an Internet Key Exchange (IKE) security association (SA).

  This condition is caused by a stale IPSec SA on the spoke.

  Workaround: Use a lower ISAKMP keepalive value, or perform the **shut/no shut** commands on the spoke tunnel.

- CSCsx15761

  The fman-fp process on a Cisco ASR 1000 Series Router reloads.

  This condition occurs when the application of an access control list (ACL) fails as a result of Ternary Content Addressable Memory (TCAM) resource exhaustion. It may be followed by removal of the failed ACLs or disconnection of the affected sessions.

  Workaround: Prevent resource exhaustion.

- CSCsx18270

  Although an administrator tag is being advertised by its Interior Gateway Routing Protocol (EIGRP) neighbor router, this tag is not showing up in the local Cisco ASR 1000 Series Router topology. This behavior causes route filtering that is based on this administrator tag to fail.

  There are no known workarounds.

- CSCsx23880

  During an RP switchover on a Cisco ASR 1000 Series Router, downstream IPv6 packets (packets that traverse the 10 Gigabit Ethernet SPA and through the Gigabit Ethernet SPAs on the access side) are dropped at the Control Plane Process (CPP) because of the IPv6NoAdj error.

  The condition only occurs when **l2tp sso** is enabled.

  Workaround: If **ipv6 spd queue max-threshold 4096** is enabled, the problem does not occur.

- CSCsx25994

  Features requiring nas-port as a username as determined by authentication, authorization, and accounting (AAA) (such as pre-auth) do not work on the standby device, causing the standby sessions to fail.

  This condition occurs because AAA calculates the IP address of the best port, which is up and active. However, because the standby device has no interface visibly active, the standby router defines the best IP address to be 0.0.0.0.

  There are no known workarounds.

- CSCsx26096

  Border Gateway Protocol (BGP) negotiation with a neighbor fails on the Cisco ASR 1000 Series Router. The following log message is present, even though AFI/SAFI is supported:

  ```
  %BGP-3-NOTIFICATION: sent to neighbor ipv4-address passive 2/8 (no supported AFI/SAFI)
  3 bytes 000101
  ```

  This condition is observed after the neighbor sends a notification with code 1/ subcode 1 (OPEN/Version Not Supported) while in the Established state. The receipt of such a notification from the neighbor results in the following message:

  ```
  %BGP-3-NOTIFICATION: received from neighbor ip-address/1 (incompatible BGP version) 0
  bytes
  ```

  Workaround: Unconfigure and then reconfigure the neighbor in question on the affected Cisco ASR 1000 Series Router. For example, if you have the following configured:

  router bgp *as* **neighbor** x.x.x.x *alternate_as*

  you would configure:

  router bgp *as* **no neighbor** x.x.x.x *alternate_as* **neighbor** x.x.x.x *alternate_as*.

- CSCsx41851

  A Cisco ASR 1000 Series Router does not mark the serial interface index on to exported data correctly. Instead, the data is marked with zero. The **show ip cache flow** command output shows the serial interface as the source and destination.

  This condition occurs under the following configuration scenario:

  - The configuration includes at least one serial interface (such as SPA-2XT3/E3).
  - NetFlow is configured on that serial interface.
  - Exporter is configured on the router.

  There are no known workarounds.

- CSCsx45412

  The fman rp process on a Cisco ASR 1000 Series Router may reset. If the fman rp process resets more than once within 30 minutes, it may cause the entire Route Processor (RP) to reset.

  There are no known workarounds.

- CSCsx46513

  A configuration of 2K IPSec sessions with 500k Network Address Translation (NAT) sessions on a Cisco ASR 1000 Series Router causes the Embedded Services Processor (ESP) to restart when traffic is started.

  Workaround: Reduce the scale of your configuration.

- CSCsx46721

  After perfuming an ISSU downgrade from Cisco IOS XE Release 2.3.0 to Cisco IOS XE Release 2.2.2 on a Cisco ASR 1000 Series Router, after an interval the IPv4 traffic stops getting encrypted and is sent as clear text.

  There are no known workarounds.

- CSCsx47069

  After a switchover is performed on a Cisco ASR 1000 Series Router, ping replies have the wrong source address.

  This issue occurs because under certain conditions Cisco Express Forwarding (CEF) may fail to inform the hardware that the source-eligible flag has changed for a specific Forwarding Information Base (FIB). FIB triggers notifications to the hardware only when the Output Chain Element (OCE) of the FIB changes.

  There are no known workarounds.

- CSCsx48349

  Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors flap on a Cisco ASR 1000 Series Router. If the neighbors are left in this state, Internet Key Exchange (IKE) may go into a non-operational state.

  This condition is observed under the following scenario:

  – Dynamic Multipoint VPN (DMVPN) hub and spokes are configured with the default Next Hop Resolution Protocol (NHRP) holdtime and EIGRP hello/update intervals.

  – 1K spokes are trying to simultaneously register to the hub immediately after the hub's router reloads.

  Workaround: 1. Reduce the number of spokes. 2. Lengthen the EIGRP hello and holdtime to 900 seconds.

- CSCsx50568

  When reconfiguring control plane policing at times of high stress to the Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router, control plane policing stops working, and all CPP dataplane updates stop.

  Workaround: Do not configure control plane policing during a time of high stress on the ESP. After this condition occurs, the only recovery seems to be a full ESP reload.

- CSCsx51695

  The Generic Routing Encapsulation (GRE) tunnel line protocol goes down after a consolidated package downgrade from Cisco IOS XE Release 2.3.0 to Cisco IOS XE Release 2.2.2.This behavior can also occur after a sub-package ISSU downgrade or upgrade between these two releases.

  During the sub-package ISSU downgrade or upgrade, all but one of the tunnels goes down, but after an interval, the tunnel recovers. In the instance of the consolidated package downgrade, the tunnel never recovers.

  There are no known workarounds.

- CSCsx51860

  In a very large Dynamic Multipoint VPN (DMVPN) network (for example, 1500 spokes connecting to a single hub), some of the tunnels may not be fully reflected in the hardware and may cause traffic drop on those tunnels.

  This condition is more likely to happen when users configure a very large number of spokes and toggle the interfaces between shut and no shut multiple times.

  Workaround: Perform **shut/no shut** on the specific spoke for which the hub does not have the entry in the hardware.

- CSCsx56379

  A Cisco ASR 1000 Series Router configured with the Session Border Controller feature, may experience a software-forced reload when multiple configuration/deconfiguration sequences of the Session Border Controller feature are executed within a short amount of time.

  There are no known workarounds.

- CSCsx60439

  A Cisco ASR 1000 Series Router that is configured with a Quality of Service (QoS) service policy on an output interface and a non-default maximum transmission unit (MTU) value may experience an unexpected reload of the Embedded Services Processor (ESP). The following error messages are returned:

  ```
  QED_QED_LDC_LEAF_INT_INT_LDC_LCOMPUTE_ENG_MAX_SCH_ERR
  PQS_PQS_LOGIC1_INTR_LEAF_INT_INT_CACHE_STATUS_TIME_OUT_ERR_D1
  ```

  Workaround: To avoid this issue, do not configure the MTU to be greater than the default MTU of the interface on which the QoS policy has been applied.

- CSCsx61701

  The Cisco ASR 1000 Series Router may reload after the Network Address Translation (NAT) High Speed Logger (HSL) is unconfigured and later re-configured.

  Workaround: When you unconfigure NAT high speed logging (v9), reload the router to prevent the risk of potential problems.

- CSCsx62253

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router reloads when a configuration change is made to the Firewall High Speed Logger (HSL).

  This condition may occur when HSL is removed using the **no log flow-export v9 udp destination** command and then re-configured using the **log flow-export v9 udp destination** command.

  Workaround: Do not remove the HSL configuration unless all of the Firewall configuration is to be removed. You can modify the HSL configuration.

- CSCsx65975

  The Cisco ASR 1000 Series Router unexpectedly resets during an in-service software upgrade (ISSU) from Cisco IOS XE Release 2.2 to Cisco IOS XE Release 2.3.

  This condition is observed only when Secure Shell (SSH) RSA keys are configured/generated.

  Workaround: Set your SSH RSA keys to zero before the ISSU and create new ones after the ISSU using the following commands.

  ```
  Router(config)#crypto key zeroize rsa
  Router(config)#crypto key generate rsa
  ```

  Further Problem Description: The router may reset unexpectedly in the IOS fast path if SSH sessions are active during the ISSU process.

- CSCsx66227

  When a 1 Gigabit Ethernet SPA is OIR removed and a 10 Gigabit Ethernet SPA is OIR inserted into the same subslot on a Cisco ASR 1000 Series Router, the 10 Gigabit Ethernet SPA interface is not able to forward traffic.

  This condition is observed when Quality of Service (QoS) is configured on the 1 Gigabit Ethernet SPA interface, and the same subslot is used for two different types of SPAs.

  Workaround: Remove the QoS Modular QoS CLI (MQC) configuration from the SPA interfaces before OIR removing the SPA. Another workaround is to reload the ESP after OIR inserting the new SPA.

- CSCsx66736

  IPSec sessions do not come up after upgrading or downgrading the Embedded Services Processor (ESP) using the ISSU sub-package for a single ESP chassis on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsx68883

  The **default-metric** (BGP) command sets the MED value of an External BGP (eBGP) route even though the command is not intended to affect eBGP routes.

  Workaround: You can override this MED value by setting this value for the route explicitly using eBGP.

- CSCsx74979

  When the Virtual Fragmentation and Reassembly (VFR) feature is enabled on a Cisco ASR 1000 Series Router, the triggering of an Internet Control Management Protocol (ICMP) redirect message by a fragmented jumbo packet that has been reassembled by VFR may, under certain conditions, cause an unexpected reset of the Embedded Services Processor (ESP).

  Workaround: Disable IP redirects on the interface on which VFR is configured by using the **no ip redirects** interface subcommand.

- CSCsx76017

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router might become stuck in boot mode. No core dump is created.

  Workaround: Reload the ESP manually.

- CSCsx76169

  On a Cisco ASR 1000 series router, fragmented jumbo frames exceeding 9216 bytes in total packet size may, under certain conditions, be dropped in the Virtual Fragmentation and Reassembly (VFR) path. The following error messages may be observed:

  ```
  %FRAG-3-REASSEMBLY_DBG: Reassembly/VFR encountered an error: VFR failed at refrag:
  need to reduce ingress VFR i/f MTU to 4470 or less
  %FRAG-3-REASSEMBLY_ERR: Reassembly/VFR encountered an error: frag info reference
  counter reaches zero
  ```

  Workaround Use the default maximum transmission unit (MTU) value or less on the interface on which VFR is enabled.

- CSCsx76862

  On a Cisco ASR 1000 Series Router with the Virtual Fragmentation and Reassembly (VFR) feature enabled, the VFR processing of fragments can get stuck, and all fragments requiring VFR processing are dropped. There is no impact on any traffic not requiring VFR processing.

  There are no known workarounds.

- CSCsx80170

  On a Cisco ASR 1000 Series Router configured with the Multicast Source Discovery Protocol (MSDP), a Reverse Path Forwarding (RPF) check on a multicast packet may fail and the multicast traffic will not be forwarded.

  There are no known workarounds.

- CSCsx99319

  A reload of the Cisco QuantumFlow Processor (QFP) on the Cisco ASR 1000 Series Router may occur when an Application Layer Gateway (ALG) such as Session Initiation Protocol (SIP), Skinny Call Control Protocol (SCCP), H.323, or File Transfer Protocol (FTP) runs with a static interface Network Address Translation (NAT) configuration.

  Workaround: Use an inside static configuration instead of a static interface configuration. For example, replace the following configuration:

  ```
  ip nat in source static 13.1.1.2 int gi0/3/0
  ```

  with the following configuration instead:

  ```
  ip nat inside source static 13.1.1.2 12.1.1.2
  ```

Resolved Caveats—Cisco IOS XE Release 2.2.3

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.2.3.

- CSCec51750

  A Cisco router that is configured for HTTP and voice-based services may reload unexpectedly because of internal memory corruption.

  There are no known workarounds.

  Note that the fix for this condition prevents the router from reloading and enables the router to generate the appropriate debug messages.

  The internal memory corruption is addressed and documented in caveat CSCec20085.

- CSCsc94969

  After configuring the **import ipv4 unicast map #name** command under the **ip vrf #name** command, all existing routes (except those direct-connected) under the VPN routing/forwarding (VRF) table disappear.

  This condition occurs when the Cisco router is configured with Multiprotocol Label Switching (MPLS), VRF, and import IPv4.

  There are no known workarounds.

- CSCse29570

  A Cisco router might unexpectedly reload during a CNS configuration download.

  This condition only occurs when the downloaded configuration disables the CNS initial or partial configuration.

  Workaround: Use static configuration and prevent configuration download from the CNS server.

- CSCsf25722

  When attempting to transfer files using Secure Copy (SCP), a Cisco router may implement a software forced reload after executing the **copy disk0**: *image name* **scp** command.

  Workaround: Do not use SCP to transfer files.

- CSCsh58099

  After a long period of uptime or frequent File Transfer Protocol (FTP) usage, the Cisco ASR 1000 Series Router will periodically log the following message:

  ```
  name_svr.proc[65]: Could not register interest for /registry/2992898759/3457843965:
  Not enough memory<31>SLOT0
  ```

  There are no known workarounds.

- CSCsj12254

  A Cisco router may reload due to a watchdog timeout when the **show interface | include AAA**, **AAA** command is issued. The following message appears on the console:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Virtual Exec
  ```

  This condition is observed only when a virtual access interface shows a very high number of renegotiations.

  Workaround: Clear the session.

- CSCsj45031

  The Cisco ASR 1000 Series Router is unable to download a file from a Tectia or Unix server using Secure Copy (SCP).

  Workaround: Use a Linux, Windows, or Secure Shell (SSH) server instead.

- CSCsk25046

  When a policy is applied on the control plane to an interface with an ifindex of 14, the corresponding entry will not appear in cbQosServicePolicyTable. This condition impacts device monitoring.

  Workaround: Remove the policy on the control plane.

- CSCsk49835

  When you apply and remove a loopback at the far-end/near-end in a multirouter-automatic protection switching (MR-APS) pair on a Cisco ASR 1000 Series Router, the protect interface always shows as looped. Even performing a **shut/no shut** on the interface/controller doesn't clear the loopback.

  This condition occurs only when the encapsulation method used is the Point-to-Point Protocol (PPP). When the encapsulation method is changed to High-Level Data Link Control (HDLC), the loopback is cleared.

  There are no known workarounds.

- CSCsl24449

  The newly active Route Processor (RP) on a Cisco ASR 1000 Series Router occasionally logs an error message and resets after the **issu runversion** command is used to switch to the updated software version on the standby RP. The logged error message is:

  ```
  ISSU-3-ERP_AGENT_SEND_MSG: IPC send for client/entity pair failed; error code is retry
  queue flush
  ```

  This condition occurs only in the Cisco IOS XE 2.2 Release.

  There are no known workarounds.

- CSCsl29214

  A Cisco ASR 1000 Series Router may encounter a bus error crash when the **show run** command is executed.

  This condition may be triggered when multiple users issue authentication, authorization, and accounting (AAA) configuration changes.

  There are no known workarounds.

- CSCsl63494

  The authentication, authorization, and accounting (AAA) server does not count active user sessions correctly. As a result, user authentication may be denied by the AAA server because the max session limit has been reached.

  This condition occurs when the user initiates X.25, Secure Shell (SSH), rsh, rlogin or Telnet sessions and later disconnects them.

  Workaround: Consider removing the max session limit.

- CSCsm50317

  Service policy counters stop updating after applying the service policy to a virtual template. The policy-map counters become stuck at zero.

  Workaround: Remove the policy and re-apply it.

- CSCsm55629

  When logging Secure Shell (SSH) events using the **ip ssh logging events** command, no user name is returned to the logs for the SSH session. This issue occurs for both the login event and the logout event.

  There are no known workarounds.

- CSCsm69981

  Intelligent Services Gateway (ISG) is not allocating the next free port in the cyclic order as expected.

  This condition is observed on PC clients using a web-portal when the browser is shutdown, a new browser is started within 60 seconds, and the web-server timeout is set for 60 seconds.

  Workaround: Adjust the web-server TCP port allocation timers to match that of the ISG and PC clients.

- CSCsm85137

  Clearing of counters or a burst amount of volume traffic can cause the GigaByte counters to be incorrectly incremented or not incremented for Intelligent Services Gateway (ISG) IP SIP sessions within authentication, authorization, and accounting (AAA) accounting records.

  There are no known workarounds.

- CSCso04657

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

  Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

- CSCso45720

  When a third-party vendor client is L2-connected to an Intelligent Services Gateway (ISG) interface and the client supports DHCP, the client will perform a DAD ARP REQ after it receives the DHCP offer. This ARP REQ uses 0.0.0.0 in the “sender-ip-address” field to which the ISG will respond. However, this response causes the third-party client to assume this IP already exists on the network, and so it sends back a DHCP decline to the DHCP server. In addition to the client failing to get an IP address, this issue can also deplete the IP address pool.

  There are no known workarounds.

- CSCso50347

  A Cisco router may reload after the **show ip bgp** *l2vpn vpls* **all prefix- list** command is issued.

  Workaround: Use the **show ip bg**p command instead.

- CSCso50671

  Clearing of counters or a burst amount of volume traffic can cause the GigaByte counters to be incorrectly incremented or not incremented for the iEdge Accounting feature within authentication, authorization, and accounting (AAA) accounting records.

  There are no known workarounds.

- CSCso82707

  If the Intelligent Services Gateway (ISG) RADIUS proxy does not receive a response for its first accounting request, it will create the session but the process will not retransmit consecutive accounting requests back to the RADIUS proxy client.

  This condition is observed when the authentication, authorization, and accounting (AAA) server goes down immediately after authentication, but before the accounting requests are sent.

  There are no known workarounds.

- CSCso90970

  When the **no ip proxy-arp** command is configured under an Intelligent Services Gateway (ISG) enabled interface, it is ignored.

  There are no known workarounds.

- CSCsq29198

  A block-allow can not be sent in same Multicast Listener Discovery (MLD) report for a Cisco ASR 1000 Series Router when the mCAC bandwidth limit is reached. Allow-block is not supported for proper mCAC bandwidth limit handling.

  There are no known workarounds.

- CSCsq31958

  In a network with a redundant topology, an Open Shortest Path First (OSPF) external route may remain stuck in the routing table after a link flap.

  Workaround: This issue can be resolved by entering the **clear ip route** command for the affected route.

- CSCsq59784

  Under extreme pressure, such as the flapping of many sessions, a Cisco router may reload.

  This condition occurs when auto-services are configured for the sessions, and there is significant session flapping, that is, session creation and clearing.

  There are no known workarounds.

- CSCsq75350

  When traffic-class based service is applied to a Point-to-Point Protocol (PPP) session using an on-box configuration or service log-on, flow accounting records (start/stop/interim) may not be generated for the PPP session.

  There are no known workarounds.

- CSCsq88370

  The **ip dhcp relay information** configuration still remains even after the interface removed.

  Workaround: Explicitly delete the **ip dhcp relay information** command before removing the interface.

- CSCsr06282

  The Cisco router reloads following a Simple Network Management Protocol (SNMP) get operation when a Dynamic Host Control Protocol (DHCP) operation is configured with option-82 parameters.

  Workaround: Do not query MIB objects relating to the DHCP operation configured with option-82.

- CSCsr29468

  Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml

- CSCsr39272

  The following SPA error has been reported:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error printed when SPA sensor temp overruns
  buffer
  ```

  There are no known workarounds.

- CSCsr51820

  Traffic is not forwarded across an IPSec-protected Generic Routing Encapsulation (GRE) tunnel on a Cisco ASR 1000 Series Router when that tunnel is a member of a virtual routing and forwarding (VRF) instance.

  This condition occurs when internal traffic is sourced from or destined to a VRF, and tunnel protection is applied on a tunnel interface whose IP address is a member of that VRF but the source and destination of the tunnel endpoints are in the global routing table.

  There are no known workarounds with tunnel-protection enabled.

- CSCsr56358

  When a Route Processor (RP) switchover is performed on the Cisco ASR 1000 Series Router under traffic load, some sessions at the new standby RP have the SSM remote session ID set to 0.

  This condition occurs in scaled configurations (for example, 16K sessions/1 tunnel established with Model D.2 QoS configuration terminated at an L2TP Access Concentrator (LAC)).

  There are no known workarounds.

- CSCsr64012

  When an IPv6 address is configured on the Session Border Controller (SBC) interface on a Cisco ASR 1000 Series Router, an InjectErr occurs periodically:

  Workaround: Disable IPv6 Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on the SBC interface using the following commands:

  ```
  interface sbc1
  no ipv6 pim
  no ipv6 mld router
  ```

  (IPv6 PIM and MLD are enabled by default and are not required.)

- CSCsr68545

  When an IP Service Level Agreement (SLA) is configured with a round-trip time (**RTT**), the following error message occurs:

  ```
  000302: Jul 24 13:00:13.575 CDT: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  -Traceback= 0x410FD1A4 0x41119DB0 0x41138324 0x41DE5714
  ```

  There are no known workarounds.

- CSCsr72527

  Per-user access control lists (ACLs) on a Cisco ASR 1000 Series Router may not install properly when they are downloaded from RADIUS servers.

  This condition can occur when PPP over X (PPPoX) sessions are being brought up.

  There are no known workarounds.

- CSCsr76893

  In a Dynamic Multipoint VPN (DMVPN) hub and spoke network all spokes are affected when one spoke sends an Internet Group Management Protocol (IGMP) leave message for the active multicast group.

  This condition occurs when the Cisco ASR 1000 Series Router is running a dual DMVPN hub and spoke network and the Route Processor (RP) and source are located behind the dual DMVPN hub routers.

  Workaround: Move the RP to the hub router.

- CSCsr94507

  Traffic loss of about 2 seconds can occur at an Asynchronous Transfer Mode (ATM) interface during the Route Processor (RP) switchover on a dual IOS High Availability (HA) configuration.

  This condition only occurs on a Cisco ASR 1004 or Cisco ASR 1002 router with a dual IOS HA configuration. This condition does not occur on a Cisco ASR1006 router.

  There are no known workarounds.

- CSCsr96049

  When a tunnel interface is configured with the **cdp enable** command on a Cisco ASR 1000 Series Router, the following error is returned:

  ```
  %SYS-2-GETBUF: Bad getbuffer, bytes= ... -Process= "Net Background", ipl= 2, pid= 43
  ```

  Workaround: Remove the **cdp enable** command on the tunnel interface.

- CSCsu26526

  A memory leak can be observed on the L2TP Network Server (LNS) when the Point-to-Point Protocol (PPP) client performs a renegotiation.

  There are no known workarounds.

- CSCsu38228

  On a Cisco ASR 1000 Series Router with Weighted Random Early Detection (WRED) enabled, when **random-detect exponential-weighting-constant** is reset with valid values (1-6, default is 4) and removed from the policy map applied, the random-detect exponential-weighting-constant is set to 9.

  Workaround: Reconfigure **random-detect exponential-weighting-constant** to the correct value.

- CSCsu40536

  The Cisco ASR 1000 Series Router reloads when it processes a non-DNS packet destined to port 53 (DNS) and Network Address Translation (NAT) is configured.

  Workaround: Apply an access control list (ACL) to drop any packets destined to port 53.

- CSCsu48898

  A Dynamic Host Control Protocol (DHCP) component may cause the Cisco router to reset every few minutes.

  There are no known workarounds.

- CSCsu50406

  When a Cisco ASR 1000 Series Router is reloaded or an online insertion and removal (OIR) insertion is performed on one of its SPAs, an error message is generated and the Quality of Service (QoS) policy is suspended.

  This condition occurs when a QoS policy is attached to the Multilink PPP (MLP) bundle that has **shape %** *n* configured where *n* is less than 13.

  Workaround: Manually remove and then reattach the QoS policy to the MLP bundle.

- CSCsu50921

  When more than 500 IPSec sessions are set up across a Dynamic Virtual Tunnel Interface (DVTI) Easy VPN (EzVPN) configuration on a Cisco ASR 1000 Series Router and these sessions are cleared and brought up again, the IPSec tunnels come up but traffic does not get through, and the Cisco QuantumFlow Processor (QFP) flows cease to exist.

  Workaround: This condition is not seen when dynamic crypto maps are used with EzVPN instead of Dynamic VTI.

- CSCsu55070

  If **no cdp enable** is configured on a few ports on a POS-OC48 SPA and the Cisco ASR 1000 Series Router is reloaded, the Cisco Discovery Protocol (CDP) gets disabled on all the ports.

  This condition occurs when the configuration is saved prior to the reload.

  Workaround: After the reload, re-enable the ports you do not want to have disabled using the **cdp enable** command.

- CSCsu72815

  When IP virtual reassembly is configured, the Cisco ASR 1000 Series Router may crash due to a fragmented IP packet.

  Workaround: Disable ip virtual reassembly.

- CSCsu83925

  The group entry displays incorrectly in the **show ipv6 mroute** command and the Protocol Independent Multicast (PIM) topology table on a Cisco ASR 1000 Series Router. This condition occurs if the value of the entry is checked immediately after sending a Multicast Listener Discovery (MLD) join. If you wait a few seconds, the expected group entry value appears in both the **show ipv6 mroute** command and the PIM topology table.

  Workaround: Wait 3 to 5 seconds before checking the value of the group entry after an MLD join.

- CSCsu84714

  When performing an **expand** on a consolidated package for the Cisco ASR 1002 router, warning messages are displayed.

  Workaround: No workaround is needed; this issue is cosmetic only and does not affect the router's operation.

- CSCsu89555

  Neighbors in a virtual routing and forwarding (VRF) instance may not be reachable on a Cisco ASR 1004 Router after a Route Processor (RP) subpackage in-service software upgrade (ISSU) and RP switchover.

  This condition can occur after an RP subpackage ISSU from Cisco IOS XE Release 2.1.2 to 2.2.1 or Cisco IOS XE Release 2.1.2 to 2.2.2.

  Workaround: Perform an ISSU rollback to the Cisco IOS XE Release 2.1.2 package.

- CSCsu93126

  When the **show platform software ip esp** [**active | standby**] **cef** command is issued, the Embedded Services Processor (ESP) may leak memory.

  Workaround: Avoid using the affected show command or restart the ESP to recover the memory after the leak has occurred.

- CSCsu95355

  When **ip unnumbered** and an Access Control List (ACL) are configured for an interface on a Cisco ASR 1000 Series Router, the ACL denies the traffic and the peer router is sent an Internet Control Management Protocol (ICMP) unreachable packet with a source IP address of zero.

  Workaround: Use a static IP address for the interface.

- CSCsu96325

  NetFlow is not able to retrieve the value of ifIndex for dot1Q subinterfaces after a Cisco ASR 1000 Series Router reload.

  Workaround: Although entering subinterface configuration mode will populate the value, it does not provide a feasible workaround.

- CSCsv04674

  The M(andatory)-Bit is not set in the Random Vector AVP of the Egress ICCN packet, which is a requirement according to RFC2661.

  There are no known workarounds.

- CSCsv06503

  IPv6 Nonstop Forwarding (NSF) convergence notification may occur before the working set of interfaces become active following an active Route Processor (RP) Stateful Switchover (SSO) failover to the standby RP.

  There are no known workarounds.

- CSCsv09347

  When the Host Standby Routing Protocol, version 2 (HSRPv2) for IPv6 is configured on both Cisco ASR 1000 Series Routers, IOSd on the standby Cisco ASR 1000 Series Router reloads when rebooting.

  There are no known workarounds.

- CSCsv09833

  IP packets larger then 1454 bytes with the “don't fragment” bit set in the IP header are not passing through an IPSec tunnel on a Cisco ASR 1000 Series Router when the maximum transmission unit (MTU) configuration of the tunnel interface and underlying physical interface should allow these packets to pass.

  This condition is observed on Cisco ASR 1000 Series Routers running Cisco IOS XE Release 2.1.x and Cisco IOS XE Release 2.2.x.

  Workaround: Decrease the IP MTU on the tunnel interface to 1454 or less. To avoid fragmentation of large TCP packets in the network, configure “**ip tcp adjust-mss 1434**” on the tunnel interface.

- CSCsv14100

  The Cisco ASR 1000 Series Router is sending some RADIUS Access-Requests and Accounting-Requests with a NAS-Port value of 0 during PPPoE session establishment. If the responding server does not respond to an Accounting-Request that has a NAS-Port value of 0, the following error messages appear on the console:

  ```
  RADIUS server 10.xx.xxx.x xxxxxxxxx is not responding.
  RADIUS server 10.xx.xxx.x xxxxxxxxx is being marked alive.
  ```

  There are no known workarounds.

- CSCsv14986

  The Cisco QuantumFlow Processor (QFP) on a Cisco ASR 1000 Series Router reloads when multiple subscribers (at a rate of 40 calls per second (CPS)) try to log on using the Spirent Avalanche tool. This condition occurs under the following configuration scenario:

  - IP session as aggregator
  - Static IP without MQC,
  - L4 Redirect with VRF web logon

  There are no known workarounds.

- CSCsv15063

  When a Point-to-Point Protocol (PPP) packet is forwarded downstream from a Cisco ASR 1000 Series Router in a Virtual Private Dialup Network (VPDN) Multihop scenario, the router is stripping the HDLC-like “0XFF03” value.

  There are no known workarounds.

- CSCsv15931

  The Route Processor (RP) on a Cisco ASR 1000 Series Router reloads in an Layer 2 Tunnel Protocol (L2TP) High Availability (HA) configuration when tunnels are cleared with **clear vpdn tunnel** command while the tunnels/session are being established.

  There are no known workarounds.

- CSCsv17521

  The Cisco ASR 1000 Series Router reloads when unconfiguring Border Gateway Protocol (BGP), access lists, and route map configurations.

  There are no known workarounds.

- CSCsv18533

  When running random packets (with invalid L7 data) with Network Address Translation (NAT) and all Application Layer Gateway (ALG) enabled on a Cisco ASR 1000 Series Router for over 24 hours, the following Cisco QuantumFlow Processor (QFP) error occurs:

  ```
  error INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0
  ```

  In addition, the ucode core file returns the following traceback:

  ```
  0x801C93C9:abort(0x801c935c) 0x6d  0x801AAFE1:rbuf_ooh_handler(0x801aaf8c) 0x55
  0x800206EC:noop(0x800206ec) 0x0  0x801C7C0F:timer_start(0x801c7ba8) 0x67
  0x801A7A3D:chunk_process_retmem_timer(0x801a7924) 0x119
  0x801C46A8:time_process_timer_ev(0x801c4644) 0x64

  0x801C64A8:process_recycle_control(0x801c6414) 0x94
  0x801C8218:mpass_restart_processing(0x801c7f14) 0x304  0x801C88B1:main(0x801c8858)
  0x59  0x80020055:_stext(0x80020000) 0x55  0x80000000:_ResetVector(0x80000000) 0x0
  ```

  There are no known workarounds.

- CSCsv22769

  In a dual IOS system operating in Route Processor Redundancy (RPR) mode on a Cisco ASR 1000 Series Router, the system unexpectedly reloads on switchover.

  There are no known workarounds.

- CSCsv30556

  Higher level applications on a Cisco ASR 1000 Series Router, such as Group Encrypted Transport VPN (GET VPN), may not receive their multicast packets.

  This condition occurs when the applications are running IPv4 multicast with Protocol Independent Multicast - Sparse Mode (PIM-SM).

  Workaround: Use PIM - Source Specific Multicast (SSM), or bidirectional PIM (bidir-PIM).

- CSCsv32313

  In a Dynamic Multipoint VPN (DMVPN) hub and spoke network all spokes are affected when one spoke sends an Internet Group Management Protocol (IGMP) leave message for the active multicast group.

  This condition occurs when the Cisco ASR 1000 Series Router is running a dual DMVPN hub and spoke network and the Route Processor (RP) and source are located behind the dual DMVPN hub routers.

  Workaround: Move the RP to the hub router.

- CSCsv38166

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

  The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS SCP client feature.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml.

- CSCsv39880

  A Cisco ASR 1000 Series Router crashes when generating a Rivest, Shamir, and Adelman (RSA) key that is not a multiple of 64.

  Workaround: Use a key that is a multiple of 64.

- CSCsv47580

  During the boot or reboot of a Cisco ASR 1000 Series Router, the management interface's (Interface Gigabit 0) line protocol is declared up even though a cable is not connected to the management interface.

  Workaround: To clear this condition, issue the **shut/no shut** command for the interface Gigabit 0 configuration.

- CSCsv52140

  When an access control list (ACL) is applied on a Cisco ASR 1000 Series Router interface with PPP over Ethernet (PPPoE) configured, the ACL reports hits on ports not used by traffic. Some traffic is unexpectedly lost.

  Workaround: Remove the access control list if traffic is affected.

- CSCsv53908

  On a Cisco ASR 1006 Router, the inventory information for the standby Route Processor (RP) in the **show inventor**y command output is not updated after the hardware replacement of standby RP.

  This information can only be recovered by a system reload; it can not be recovered by online insertion and removal (OIR) of the standby RP, or a reload of the standby RP and an RP switchover.

  There are no known workarounds.

- CSCsv58823

  The Cisco QuantumFlow Processor (QFP) driver process on a Cisco ASR 1000 Series Router causes high CPU usage on the forwarding processor.

  This condition occurs when the Cisco QFP driver does not completely process Ternary Content Addressable Memory (TCAM) parity errors, leading to the high CPU usage. This condition also prevents subsequent TCAM parity errors from being corrected.

  Workaround: To resolve the issue, reset the forwarding processor.

- CSCsv60491

  Real-Time Control Protocol (RTCP) flows corresponding to media flows belonging to Session Border Control calls on a Cisco ASR 1000 Series Router can now be policed using a Maximum Burst Size (MBS) equal to the MBS of the associated RTP flow.

  There are no known workarounds.

- CSCsv61175

  Under rare timing conditions, when running Session Initiation Protocol (SIP) traffic through Network Address Translation (NAT) on the Cisco ASR 1000 Series Router, the Cisco QuantumFlow Processor (QFP) may reload.

  There are no known workarounds.

- CSCsv64188

  When **negotiation auto** is configured on both management ethernet ports on a Cisco ASR 1000 Series Router, the line protocol is down.

  Workaround: Change the configuration to **no negotiation auto** and fix the speed and duplex.

- CSCsv64997

  High CPU utilization occurs on the Linux kernel on a Cisco ASR 1000 Series Router.

  The CPU utilization on Linux kernel can be confirmed by using the **monitor platform software process** *fru* command.

  Workaround: Reload the field replaceable unit (FRU).

- CSCsv73388

  The circuit-id-tag and remote-id-tag attributes might be duplicated in packets sent to the RADIUS server.

  There are no known workarounds.

- CSCsv73509

  If **no aaa new-model** is configured by EXEC users, authentication occurs through the local login even when TACACS is configured.

  This condition is observed under a VTY configuration.

  There are no known workarounds.

- CSCsv80892

  The Cisco IOS process restarts on the Cisco ASR 1000 Series Router after the following watchdog error is generated:

  ```
  ASR1000-WATCHDOG: Process = Modem Autoconfigure -Traceback=
  1#66917119eb43e6762c3a667a957013f9 c:BBF8000+C1020 c:BBF8000+C1020 :10000000+BE0524
  :10000000+19E382C :10000000+19E4408
  ```

  This condition occurs when there is nothing connected to the aux port and the aux port is configured with the following commands:

  ```
  modem InOut
  modem autoconfigure discovery
  flowcontrol hardware
  ```

  Either the cable is disconnected from the router, or the cab.le is not connected to a peripheral device.

  Workaround: Connect the aux port to a peripheral device.

- CSCsv85639

  When the TCP adjust MSS feature is configured under a Virtual-Template interface used to establish L2TP sessions on a Cisco ASR 1000 Series Router that is functioning as an L2TP Network Service (LNS), the system goes out of service.

  Workaround: Unconfigure the TCP adjust MSS feature using the **no ip tcp adjust-mss** command.

- CSCsv86561

  A Cisco ASR 1000 Series Router reloads at Quality of Service (QoS) drop policy.

  There are no known workarounds.

- CSCsv86784

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may unexpectedly reload when removing NetFlow from an interface with traffic using the following interface configuration commands:

  ```
  no ip flow
  no ip flow egress
  no flow sampler sampler-name
  no flow sampler sampler-name egress
  ```

  Workaround: To avoid this issue, execute the **shutdown** command on the interface before removing the NetFlow configuration.

- CSCsv87997

  The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay process resets on the Active Route Processor (RP).

  There are no known workarounds.

- CSCsv92307

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may see a spike or constant high CPU usage when the ESP is reloaded and a large number of routes and multicast entries are enabled.

  Workaround: Do not perform an ESP reload or reload the ESP using the Route Processor (RP) when these symptom occur.

- CSCsv93452

  A SPA interface processor (SIP) card on a Cisco ASR 1000 Series Router may experience unexpected reloads when MAC accounting is configured.

  Workaround: The only known workaround is to disable MAC accounting.

- CSCsv94909

  When a certain class of Internet Control Management Protocol (ICMP) frames are received and not handled properly by Network Address Translation (NAT) on the Cisco ASR 1000 Series Router, the Embedded Services Processor may reload.

  Workaround: Create the following access control list (ACL) and apply it to incoming packets on all inside and outside NAT interfaces:

```
ip access ext num
permit tcp any any
permit udp any any
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any timestamp-request
permit icmp any any timestamp-reply
permit icmp any any unreachable
permit icmp any any source-quench
permit icmp any any redirect
permit icmp any any time-exceeded
permit icmp any any parameter-problem
deny icmp any any
```

- CSCsv95826

  Single bit errors (SBEs) detected on the Cisco QuantumFlow Processor (QFP) driver cause the Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router to reload.

  There are no known workarounds.

- CSCsv98491

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router unexpectedly reloads for some types of IPv4 options packet with uncommon alignments.

  Workaround: Configure the router to ignore or drop IPv4 options using the **ip options** command as follows:

```
Router(config)# ip options ?
  drop Drop all IP options packets
  ignore Ignore options in IP options packets
```

- CSCsv99429

  When Open Shortest Path First (OSPF) neighbors on a Cisco ASR 1000 Series Router are configured with fast hellos, the neighbors flap when the **write memory** command is executed or the value of **config-register** is changed.

  Workaround: Copy the running configuration to harddisk first. For example:

```
Router#copy running-config harddisk:run.conf
Destination filename [run.conf]?
8695 bytes copied in 0.258 secs (33702 bytes/sec)
Router#copy harddisk:run.conf startup-config
Destination filename [startup-config]?
[OK]
8695 bytes copied in 7.507 secs (1158 bytes/sec)
```

  Further Problem Description: The **write memory** problem is no longer issue in Cisco IOS XE Release 2.2.3. The **config-register** problem will be addressed in CSCsx59262.

- CSCsw14643

  Although the Auto-RP cache is populated initially when the first RP discovery packet arrives (allowing Protocol Independent Multicast - Sparse Mode (PIM-SM) to function), subsequent packets are lost, causing the Auto-RP cache to expire and disrupting PIM-SM connectivity.

  This condition occurs because the Cisco ASR 1000 Series Router has selected a loopback interface to join the Auto- RP discovery group.

  Workaround: Remove the loopback interface from the configuration and then add the loopback interface back in the configuration.

- CSCsw18583

  The Cisco ASR 1000 Series Router restarts when an access-control type policy map is applied to a 10 gigabit subinterface with no traffic running.

  There are no known workarounds.

- CSCsw21000

  The active Route Processor (RP) on a Cisco ASR 1000 Series Router reloads with core/crashinfo because of an abnormal Dynamic Host Configuration Protocol version 4 (DHCPv4) sequence.

  This condition occurs when the router is configured as a DHCP relay agent with 8k VLAN and 8 port-channels. There is no other traffic or stress.

  There are no known workarounds.

- CSCsw21831

  Embedded Services Processor (ESP) memory leakage occurs on the Cisco ASR 1000 Series Router without any traffic.

  This condition is indicated by mismatched internal ref counter values.

  There are no known workarounds.

- CSCsw22120

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload because of Network Address Translation (NAT) and multicast configuration issues.

  There are no known workarounds.

- CSCsw25478

  Auto-RP packets are consumed locally by the Cisco ASR 1000 Series Router but are not forwarded to other routers. In the routers missing these packets, the RP-mapping database is missing the group-to-RP mappings.

  This condition occurs when Auto-RP is active, and the Cisco ASR 1000 Series Router is a forwarding router for Auto-RP packets.

  Workaround: Use an alternative mechanism in place of Auto-RP.

- CSCsw25750

  Hardware encryption is inactive when there is an active Embedded Services Processor (ESP) in slot 1 of a Cisco ASR 1000 Series Router. This condition occurs in two scenarios:

  1. When both peers have active ESPs in slot1(ESP1). In this case, traffic passes through the ESP but there are no tunnels active (that is, clear text traffic passes).
  2. When one of the peers has the active ESP in slot 1, and the other peer has an active ESP in slot 0. In this case, the peer with the active ESP in slot 1 will have inactive encryption, while the peer with the active ESP in slot 0 will have active encryption. As a result, the IKE SA is active on one peer but not the other, and traffic is getting dropped.

  Workaround: Make ESP0 the active ESP in both peers.

- CSCsw28547

  An Embedded Services Processor (ESP) may reload because of invalid handling of an Internet Control Management Protocol (ICMP) packet.

  Workaround: Create the following access control list (ACL) and apply it to incoming packets on all inside and outside Network Address Translation (NAT) interfaces:

```
ip access ext num
permit tcp any any
permit udp any any
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any timestamp-request
permit icmp any any timestamp-reply
deny icmp any any
```

- CSCsw33573

  On a Cisco ASR 1000 Series Router with Quality of Service (QoS) configured on multiple interfaces, a very small memory leak (of approximately 200 bytes) may be observed when multiple service policies are configured and deleted.

  There are no known workarounds.

- CSCsw33702

  On a Cisco ASR 1000 Series Router configured with IPv6 access control lists (ACLs), memory leakage is observed on the Embedded Services Processor (ESP). This memory leak does not seem to have any adverse impact on system operation under normal deployment conditions.

  There are no known workarounds

- CSCsw33723

  A small memory leak in the smand process occurs every time the [**show | set | clear**] **platform** [**software | hardware**] or **show ip nat translations** command is executed on a Cisco ASR 1000 Series Router. The greater the command output, the faster the leak will be. Under normal operations this leak will not cause any problems. However, if an environment has been configured such that a

series of these commands are left running continuously over a long period of time, the memory leak can increment, eventually causing the process to run out of memory and crash with the following message:

```
%PLATFORM-3-ELEMENT_CRITICAL: R0/0: smand: RP/0: Committed Memory value n exceeds
critical level m
```

Workaround: Possible workarounds include the following:

- For commands with very large outputs, such as the **show ip nat translations verbose** command, which can display tens of thousands of NAT entries, try using another means for gathering the information, such as Simple Network Management Protocol (SNMP) or NetFlow export.
- Periodically restart the smand process using the **test platform software process exit shell-manager RP active stateless** command. The frequency with which the process should be restarted should not be less than a thirty minute period and will depend on how frequently the impacted commands are executed. The smand process size can be tracked using the **show platform software process list RP active name smand** command.
- The issue can be mitigated by reducing the frequency with which long running scripts containing the impacted commands are being executed. Reducing this frequency, in combination with a process restart, may keep the problem under control.

- CSCsw34175

  A Cisco ASR 1000 Series Router with Session Border Controller (SBC) configured may experience an unforced system reload if it receives a MODIFY MEGACO message containing only an AUDIT component from an attached Media Gateway Controller (MGC).

  Workaround: Do not allow the attached MGC to send a MODIFY message with an AUDIT being the only component to the message.

- CSCsw36300

  An Embedded Services Processor (ESP) on Cisco ASR 1000 Series Router may reload during the system reboot or ESP switchover.

  Workaround: The auto-reboot of the ESP should succeed.

- CSCsw36322

  The Embedded Services Processor (ESP) control process on a Cisco ASR 1000 Series Router can experience a small memory leak when the following **show** commands are issued on the ESP:

  - **show platform software ip fp** [**active** | **standby**] **cef**
  - **show platform software ip fp** [**active** | **standby**] **mfib**
  - **show platform software ipv6 fp** [**active** | **standby**] **cef**
  - **show platform software ipv6 fp** [**active** | **standby**] **mfib**

  Workaround: Avoid issuing the commands.

- CSCsw38227

  The cached memory of the active Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router is increased incorrectly when the **monitor platform software process fp active** command is issued repeatedly.

  There are no known workarounds.

- CSCsw40048

  The **vpdn logging** command can not be turned off by the **no vpdn logging** command.

  Workaround: Issue the **no vpdn logging cause normal** command and then issue the **no vpdn logging** command.

- CSCsw40607

  Session Initiation Protocol (SIP)/Session Description Protocol (SDP) messages having a route header that requires Network Address Translation (NAT) of the IP address may not be translated correctly. Any SIP message going through the Cisco ASR 1000 Series Router with a route header that requires translation could be affected by this problem.

  There are no known workarounds.

- CSCsw40203

  The Cisco ASR 1000 Series Router resets when receiving an ISAKMP/IKE packet.

  There are no known workarounds.

- CSCsw40991

  In rare circumstances, when running Network Address Translation (NAT) on a Cisco ASR 1000 Series Router, the Embedded Services Processor (ESP) reloads.

  There are no known workarounds.

- CSCsw41411

  When a NetFlow configuration is removed after a sub-package ISSU upgrade or downgrade, a Cisco ASR 1006 Router may unexpectedly generate a core file due to watchdog timer expiry.

  There are no known workarounds.

- CSCsw48224

  On a Cisco ASR 1000 Series Router, when the Packet-over-SONET (POS) interface encapsulation type is changed from Point-to-Point Protocol (PPP) to High-Level Data Link Control (HDLC), or vice-versa, and a large packet that needs fragmentation is sent immediately over the link, the Embedded Services Processor (ESP) may reload.

  There are no known workarounds.

- CSCsw74470

  On a Cisco ASR 1000 Series Router running as an L2TP Network Server (LNS), when a session has more than 4294967296 bytes downloaded or uploaded, the Gigawords RADIUS accounting attributes (52 and 53) are not being correctly incremented and sent, and the **show counters overflow** command is not reporting the correct byte count.

  There are no known workarounds.

- CSCsw75040

  Border Gateway Protocol (BGP) prefixes stop getting installed if the Cisco ASR 1000 Series Router is configured as a route-reflector and route-maps are configured in BGP.

  Workaround: Either re-apply the route-maps using the **neighbor** *x.x.x.x* **route-map y in** command, or re-apply the commands in the route-map definition and then clear the session.

- CSCsw75233

  A Cisco ASR 1002 Router that is configured as an L2TP Network Server (LNS) resets at the L2TP management daemon process with the following error message:

  ```
  %L2TUN-3-ILLEGAL: Failed to insert into socket DB
  %L2TP-3-ILLEGAL: B0D0B0D:_____:0000CF2C: ERROR: Unable to associate L2TP session with
  socket handle
  ```

  There are no known workarounds.

- CSCsw75411

  Configuring the export of NetFlow V9 statistics or sampler options data may cause all NetFlow exporting to stop and eventually cause the Cisco ASR 1000 Series Router to reload.

  Workaround: Disable the exporting of NetFlow options data using the following commands.

  ```
  no ip flow-export version 9
  no ip flow-export template options refresh-rate
  no ip flow-export template options timeout-rate
  no ip flow-export template options export-stats
  no ip flow-export template options sampler
  ip flow-export version 9
  ```

- CSCsw76109

  Next Hop Resolution Protocol (NHRP) registration fails when virtual routing and forwarding (VRF) is configured on the Dynamic Multipoint VPN (DMVPN) tunnel.

  There are no known workarounds.

- CSCsw78939

  No new sessions can be established after using a Virtual Private Dialup Network (VPDN) for a few days.

  There are no known workarounds.

- CSCsw96303

  The Route Processor (RP) on a Cisco ASR 1000 Series Router reloads unexpectedly when a GET VPN group member is configured. A fault is detected at iosd_arpa_process_packet.

  This condition occurs because of a duplication of the keyserver/group member on the same network.

  Workaround: Verify that group member/keyserver IP addresses are unique for the network.

- CSCsw98381

  Border Gateway Protocol (BGP) sessions flap after a crypto map is applied to the tunnel source interface of a Generic Routing Encapsulation (GRE) tunnel on a Cisco ASR 1000 Series Router.

  This condition is observed with as few as 500 BGP IPv4 sessions. The keepalive messages are lost and the BGP hold-time timer expires. Different sessions go down.

  Workaround: Set the tunnel **ip mtu** size to a value less than the interface maximum transmission unit (MTU). The value should be less than or equal to the size of all the headers added to the packet by the features configured on these interfaces such as GRE and IPSec. For example, if the interface MTU is 1500, set the tunnel **ip mtu** to 1400.

- CSCsw99067

  After the Cisco ASR 1000 Series Router is reloaded, Internet Security Association and Key Management Protocol (ISAKMP) renegotiation does not start anymore. No ISAKMP security associations (SAs) are created.

  This condition occurs when a dynamic crypto map is used and “gre” packets are matched in the dynamic crypto map access control list (ACL).

  For example:

```
crypto dynamic-map MPLS-SPOKES 1
  set transform-set TS
  match address MPLS-SPOKE-ACL

crypto map MPLS 2 ipsec-isakmp dynamic MPLS-SPOKES
 ip access-list extended MPLS-SPOKE-ACL
   permit gre 192.168.0.0 0.0.255.255 host 192.168.1.2
```

  Workaround: Remove the crypto map from any interfaces and reload. After reloading, re-add the crypto map.

- CSCsx03219

  A Cisco router allows less sessions then configured.

  This condition is observed when a PPPoE Active Discovery Request (PADR) is sent that has a size greater than that supported (currently 544 octets). The router counts the session as active despite it been dropped by PPPoE.

  There are no known workarounds.

- CSCsx06021

  Auto-RP information that is received and cached on a Cisco ASR 1000 Series Router configured as the stub router of a DMVPN network is not propagated to the spoke sites.

  This condition is observed when **ip pim autorp listener** and **ip pim sparse mode** are configured throughout the network, and the Auto-RP mapping agent is configured inside the main site away from the DMVPN stub router.

  Workaround: Configure a default Protocol Independent Multicast (PIM) rendezvous point (RP) for the Auto-RP groups, and turn on the local Auto-RP group sparse mode.

- CSCsx07225

  Under rare, unexpected conditions an Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload.

  There are no known workarounds.

- CSCsx14984

  On a Cisco ASR 1000 Series Router configured as Session Border Controller (SBC) data border element (DBE) with more than 100 pinholes and **deactivation-mode normal** (the default), the DBE resets when it is deactivated.

  A reset does not occur when **deactivation-mode abort** is configured.

  Workaround: Use the **deactivation-mode abort** configuration instead.

- CSCsx17676

  The Cisco ASR 1000 Series Router resets when it receives invalid fragmented IPv6 packets with extension headers that do not follow the RFC recommendation.

  There are no known workarounds.

- CSCsx35393

  The Cisco ASR 1000 Series Router may reset when Network Address Translation (NAT) and /or Firewall is enabled with H.323 traffic.

  There are no known workarounds.

- CSCsx52309

  The Cisco ASR 1000 Series Router may unexpectedly reload when a hierarchical policy-map is configured and Multicast is enabled on the router.

  This condition is observed when the interface is configured with Quality of Service (QoS) and both multicast and unicast traffic are passing through the router.

  There are no known workarounds.

- CSCsx57899

  The Embedded Services Processor (ESP) on a Cisco ASR 1002 Router reloads when multicast and Unicast traffic is sent.

  There are no known workarounds.

- CSCsx63929

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router reloads with the following Cisco QuantumFlow Processor (QFP) fatal interrupt:

  ```
  GTRMP_GTR_OTHER_LEAF_INT_INT_SDMA_VITAL_SW_ERR
  ```

  This condition is observed when IP virtual fragment reassembly (VFR) is enabled on the interface(s) and the fragmented packets are relatively large. This condition is typically caused when the maximum transmission unit (MTU) of the VFR-enabled interface is in the range of 4608 to 9216. A ping to or from the above interface may cause the error.

  Workaround: Configure the VFR-enabled interface MTU value to be 4470 or less.

- CSCsx64746

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may unexpectedly reload in certain dynamic reconfiguration scenarios involving moving from NetFlow v5 to NetFlow v9 and making an additional configuration change.

  This reload may be observed in scenarios such as the following:

  1. The exporter version is toggled from v5 to v9 with the origin-as option enabled.
  2. The exporter version is toggled from v5 to v9, NetFlow is disabled on the interface, and subsequently the NetFlow mode is re-enabled from **full netflow** to **random sampling** on that same interface, or vice-versa.

  Workaround: There are two possible workarounds for this problem:

  1. Change either the NetFlow mode (from **full netflow** to **random sampling**, or vice-versa) or the export version (from version 5 to 9, or vice-versa) BUT not both settings.
  2. If you really need to change both of these two settings, change them in this order: (a) NetFlow mode, then (b) export version. This workaround can only be executed successfully one time. Subsequent changes may cause the ESP to reload.

Open Caveats—Cisco IOS XE Release 2.2.2

This section documents possible unexpected behavior by Cisco IOS XE Release 2.2.2.

- CSCsj78195

  The **ip nat inside source static network** command allows route maps to be configured when defining static network translations on a Cisco ASR 1000 Series Router.

  The current implementation of NAT and route maps does not support the use of route maps with a static network translation, therefore the command should not allow this configuration.

- CSCsl24449

  The newly active route processor (RP) on a Cisco ASR 1000 Series Router occasionally logs an error message and resets after the **issu runversion** command is used to switch to the updated software version on the standby RP. The logged error message is:

  ```
  ISSU-3-ERP_AGENT_SEND_MSG: IPC send for client/entity pair failed; error code is retry
  queue flush
  ```

  This condition occurs only in the Cisco IOS XE 2.2 Release.

  There are no known workarounds.

- CSCsm98756

  CPU usage peaks at 99 percent for a sustained period when the **show run | inc ipv6 route** command is issued with a large-scale configuration (thousands of VLANs) on a Cisco ASR 1000 Series Router. In addition, various control plane functions such as Session Border Controller (SBC) call setup may not function as expected.

  Workaround: Redirect the **show run** command output to a file for post-processing, or save the running configuration to the startup-configuration on the bootflash and then view the running configuration by executing the s**how configuration** command from the IOS console.

- CSCso18963

  When one or more aggregation flow record formats are configured on a Cisco ASR 1000 Series Router and NetFlow is disabled, the Embedded Services Processor (ESP) may unexpectedly reload and return a message similar to the following:

  ```
  *Mar 17 02:27:12.787: %IOSXE-3-PLATFORM: F0: cpp_cp: CPP:00 Thread:116
  TS:00000000411663712433 %FNF_PROXY-3-EXPORT_INIT: Failed with return code: 1
  -Traceback= 801effa4 800552e0 80055582 8002da8d 8002dd4c 8002ea88 8003a9f4 80040476
  ```

  This condition has been observed in a configuration scenario similar to the following:

  ```
  Router(config)#interface FastEthernet0/3/1
  Router(config-if)#no ip route-cache flow
  Router(config-if)#
  *Mar 17 02:28:36.286: %CPPHA-3-FAULT: F0: cpp_ha:  CPP 0
  fault:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR class:OTHER sev:FATAL idx:1995
  cppstate:RUNNING res:UNKNOWN flags:0x7 cdmflags:0x0
  *Mar 17 02:28:36.286: %CPPHA-3-FAULTCRASH: F0: cpp_ha:  CPP 0 unresolved fault
  detected, initiating crash dump.
  *Mar 17 02:28:36.287: %CPPDRV-6-INTR: F0:
  /tmp/sw/fp/0/0/fp/mount/usr/cpp/bin/cpp_driver[4641]:  CPP10(0) Interrupt :  Mar 17
  02:28:36.277628: :INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0
  *Mar 17 02:28:36.567: %ASR1000_OIR-6-OFFLINECARD: Card (fp) offline in slot F0
  *Mar 17 02:28:37.234: %CPPDRV-3-LOCKDOWN: F0: cpp_cp:  CPP10(0) CPP Driver LOCKDOWN
  due to fatal error.
  *Mar 17 02:28:37.235: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp:  cpp_cp encountered an
  error
  ```

Note that this condition only occurs when NetFlow with export is configured. This condition will not occur in NetFlow configurations without export configured.

Workaround: Do not disable NetFlow after it has been configured.

- CSCso41804

  When global IP multicast routing is not enabled, but a Protocol Independent Multicast (PIM) rendezvous point (RP) is configured on a Cisco ASR 1000 Series Router, the standby console displays an error message about a bidir RP DF sync failure.

  Workaround: Remove the PIM RP configuration if multicast routing is not globally enabled, or enable multicast routing before adding the PIM configuration.

- CSCsq37627

  When reloading a Cisco ASR 1000 Series Router with a crypto map definition applied to two interfaces, removing the crypto map definition (using the **no crypto map** command) from the primary interface may reset the Embedded Services Processor (ESP).

  Workaround: Apply the crypto map definition to the interfaces after the reload.

  Further Problem Description: This problem occurred after removing the crypto map definition from a tunnel interface, which happened to be the primary interface. (The primary interface is the first interface that is used in spd_if_bind_a() after a reload.)

- CSCsr00490

  On a Cisco ASR 1000 Series Router with random detect configured, if a policy map is attached to multiple interfaces/parent policies, each instance shares the same Weighted Random Early Detection (WRED) threshold information. This behavior is not a problem if all attachment points are the same speed. However, if the policy map is attached to attachment points of different speeds (such as two different interface types or parent policies), the WRED thresholds shared may be inappropriate for one or more instances and may lead to unexpected drop behavior.

  This condition occurs because the control plane calculates default WRED curves based on the interface bandwidth and currently only supports one curve per class per policy map.

  Workaround: Configure a unique policy map for each speed instance/interface type or parent policy that is required. In other words, if you have a policy map “p” applied to a Gigabit Ethernet interface, with random-detect applied, that policy map should only be applied to like interfaces. If you want to configure another interface type with the same policy map, you should create another policy map “p2”, which is identical to “p1” except in name, and apply that policy map to the new interface type.

- CSCsr01097

  New Skinny Call Control Protocol (SCCP) and H.323 protocol calls can not be made after a prolonged run of traffic with these protocols on a Cisco ASR 1000 Series Router.

  This condition occurs because memory consumption in the Cisco QuantumFlow Processor (QFP) builds up, leaving no free space for new calls.

  Workaround: If you clear the calls using the **clear zone inspect session** command, you may be able to run traffic for a longer duration.

- CSCsr10774

  Clearing 16K subscriber sessions (using the **clear ip subscriber** command) on a Cisco ASR 1000 Series Router can, upon occasion, take up to 10 minutes, particularly if the sessions have Quality of Service (QoS) configured.

  The **show subscriber statistics** command indicates the sessions are gone but the **show platform hardware cpp active feature ess session | include current** command indicates the sessions are still present. It takes approximately 10 minutes to clear the sessions, and tracebacks (cpp_ess_ea_ipsub_l2_remove_hash_elem) appear during the teardown process.

  Workaround: Remove any QoS configuration from the session before clearing subscriber sessions.

- CSCsr18279

  In rare conditions, when bidirectional forwarding detection (BFD) is shut down on the Cisco ASR 1000 Series Router, a harmless traceback error message is printed.

  There are no known workarounds.

- CSCsr72674

  When a Multiprotocol Label Switching (MPLS) virtual private network (VPN) is enabled over a Generic Routing Encapsulation (GRE) tunnel on a Cisco ASR 1000 Series Router and that tunnel is configured to be associated with a user-configured virtual routing and forwarding (VRF) instance, the route processor (RP) may encounter a software exception and reload.

  There are no known workarounds.

- CSCsr72527

  Per-user ACLs on a Cisco ASR 1000 Series Router may not install properly when they are downloaded from RADIUS servers.

  This condition can occur when PPP over X (PPPoX) sessions are being brought up.

  There are no known workarounds.

- CSCsr85028

  Under rare conditions, when executing a **write memory** command on the active route processor (RP) on a Cisco ASR 1000 Series Router, the standby RP fails to synchronize the configuration from the active RP and is forced to reload. After the forced reload, the standby RP comes up, achieves Stateful Switchover (SSO), and operates as expected.

  There are no known workarounds.

- CSCsr90357

  With continuous adds and deletes of port channel interfaces, the Embedded Services Processor (ESP) software on a Cisco ASR 1000 Series Router may allocate more memory than it frees, causing it to run out of memory. This condition was observed when port channels were continuously added and deleted every half hour for more than 72 hours. Even after 72 hours the ESP stayed up.

  There are no known workarounds.

- CSCsr96049

  When a tunnel interface is configured with the **cdp enable** command on a Cisco ASR 1000 Series Router, the following error is returned:

  ```
  %SYS-2-GETBUF: Bad getbuffer, bytes= ... -Process= "Net Background", ipl= 2, pid= 43
  ```

  Workaround: Remove the **cdp enable** command on the tunnel interface.

- CSCsr96219

  A Cisco ASR 1000 Series Router configured with ip virtual-reassembly, ip nat outside, and frame relay fragmentation on an interface/subinterface generates the following error message:

  ```
  %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread:044 TS:00000004308774891044
  %ATTN-3-SYNC_TIMEOUT: msecs since last timeout 4304017, missing packets 1
  ```

  The error message does not necessarily mean a packet is physically missing; it can indicate an internal bug of packet tracking in the system.

  There are no known workarounds.

- CSCsr97633

  External BGP (eBGP) neighbors on a Cisco ASR 1000 Series Router configured with graceful restart get stuck in the OpenSent state after a route processor (RP) switchover until the hold-time expires.

  This condition causes traffic drop.

  There are no known workarounds.

- CSCsu06783

  When using a scaled Policy Based Routing (PBR) configuration with a large number of subinterfaces and Border Gateway Protocol (BGP) sessions on a Cisco ASR 1000 Series Router, the BGP sessions go down.

  This condition is observed under the following scenario:

  - When a large PBR configuration (of several hundred route maps) is used with several hundred subinterfaces.
  - When the IP virtual routing and forwarding (VRF) selection feature is also configured on the subinterfaces and route-map.
  - When several hundred BGP sessions are in use.

  There are no known workarounds.

- CSCsu35640

  The route processor (RP) on a Cisco ASR 1000 Series Router resets with following traceback when the **ip pim send-rp-discovery** command is unconfigured in global configuration mode:

  ```
  ASR1000-WATCHDOG: Process = Exec
  ```

  This condition occurs when the router is configured for PPP Terminated Aggregation (PTA) and per session multicast traffic, and 4K or 8K PPP over Ethernet (PPPoE) sessions are up.

  Workaround: Do not unconfigure the **ip pim send-rp-discovery** command in global configuration mode when 4K or 8K PPPoE sessions are up.

- CSCsu38228

  On a Cisco ASR 1000 Series Router with Weighted Random Early Detection (WRED) enabled, when **random-detect exponential-weighting-constant** is reset with valid values (1-6, default is 4) and removed from the policy map applied, the random-detect exponential-weighting-constant is set to 9.

  Workaround: Reconfigure **random-detect exponential-weighting-constant** to the correct value.

- CSCsu44557

  On a Cisco ASR 1000 Series Router, the memory allocation for Border Gateway Protocol (BGP) processes on the route processor (R) increases after clearing BGP sessions. In addition, the BGP summary counter is also incorrectly incremented.

  There are no known workarounds.

- CSCsu47716

  Point-to-Point Protocol (PPP) session disconnects occur on a Cisco ASR 1000 Series Router because of Link Control Protocol (LCP) negotiation failures. The sessions eventually do come up.

  There are no known workarounds.

- CSCsu48364

  A Quality of Service (QoS) configuration does not get successfully installed in the Cisco QuantumFlow Processor (QFP) on a Cisco ASR 1000 Series Router after a route processor (RP) switchover. Tracebacks of the form FMFP-3-OBJ_DWNLD_TO_CPP_FAILED are observed on the IOS console.

  This condition occurs in scaled scenarios, such as 16K sessions/ 8K tunnels established with a Model D.2 QoS configuration.

  There are no known workarounds.

- CSCsu50406

  When a Cisco ASR 1000 Series Router is reloaded or an online insertion and removal (OIR) insertion is performed on one of its SPAs, an error message is generated and the Quality of Service (QoS) policy is suspended.

  This condition occurs when a QoS policy is attached to the Multilink PPP (MLP) bundle that has **shape %** *n* configured where *n* is less than 13.

  Workaround: Manually remove and then reattach the QoS policy to the MLP bundle.

- CSCsu50921

  When more than 500 IPSec sessions are set up across a Dynamic Virtual Tunnel Interface (DVTI) Easy VPN (EzVPN) configuration on a Cisco ASR 1000 Series Router and these sessions are cleared and brought up again, the IPSec tunnels come up but traffic does not get through, and the Cisco QuantumFlow Processor (QFP) flows cease to exist.

  Workaround: This condition is not seen when dynamic crypto maps are used with EzVPN instead of Dynamic VTI.

- CSCsu70289

  Protocol Independent Multicast (PIM) sparse mode (PIM-SM) multicast entries are not cleared from the Multicast Routing Information Base (MRIB)/Multicast Forwarding Information Base (MFIB) when the RP mapping mode is changed to bidir mode on a Cisco ASR 1000 Series Router.

  Workaround: Execute the **clear ip mroute *** command to clear the entries.

- CSCsu72541

  On a Cisco ASR 1000 Series Router, multiple Embedded Services Processor (ESP) resets, followed by a route processor (RP) reload, are observed under the following conditions:

  - 16K sessions, PPP Termination and Aggregation (PTA) sessions up with 2 traffic class/session
  - 32K traffic classes total
  - Sessions have VRF ID and 16K sessions have been split over 20 VRFs
  - Sessions timeout 12 hours
  - No traffic flowing through the sessions

  There are no known workarounds.

- CSCsu75596

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reset if a neighboring interface with Open Shortest Path First (OSPF) over Generic Routing Encapsulation (GRE)/Frame Relay (FR) goes down.

  This condition occurs when the **shutdown** command is executed on a serial subinterface used for GRE and OSPF.

  Workaround: Remove OSPF and stop traffic before executing the **shutdown** command on the subinterface.

- CSCsu80130

  The following Dynamic Host Configuration Protocol (DHCP) related traceback error messages are reported when multiple subscribers trying to log on to the web server using the Avalanche tool on a Cisco ASR 1000 Series Router:

  ```
  IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!)
  ```

  This condition occurs under the following configuration scenario:

  - Unclassified IP session with DHCP L2 access
  - L4 Redirect to portal (broadhop SME)
  - VRF
  - ISG as DHCP relay (to CNR)

  There are no known workarounds.

- CSCsu80736

  A back-to-back ping with a datagram size of more than 11862 bytes fails on a Cisco ASR 1000 Series Router with the SPA-8xCHT1/E1.

  Workaround: Increase the maximum transmission unit (MTU) size.

- CSCsu88004

  Neighbors in a virtual routing and forwarding (VRF) instance may not be reachable on a Cisco ASR 1004 Router after a route processor (RP) subpackage in-service software upgrade (ISSU) and RP switchover.

  This condition can occur after an RP subpackage ISSU from Cisco IOS XE Release 2.1.2 to 2.2.1 or Cisco IOS XE Release 2.1.2 to 2.2.2.

  Workaround: Perform an ISSU rollback to the Cisco IOS XE Release 2.1.2 package.

- CSCsu89555

  Neighbors in a virtual routing and forwarding (VRF) instance may not be reachable on a Cisco ASR 1004 Router after a route processor (RP) subpackage in-service software upgrade (ISSU) and RP switchover.

  This condition can occur after an RP subpackage ISSU from Cisco IOS XE Release 2.1.2 to 2.2.1 or Cisco IOS XE Release 2.1.2 to 2.2.2.

  Workaround: Perform an ISSU rollback to the Cisco IOS XE Release 2.1.2 package.

- CSCsu93848

  The Cisco ASR 1000 Series Router loses a Generic Routing Encapsulation (GRE) tunnel configuration and network connectivity after a route processor (RP) switchover.

  There are no known workarounds.

- CSCsv01783

  The Border Gateway Protocol (BGP) can take 1.5 minutes longer than expected to import some of the Virtual Private Network Version 4 (VPNv4) routes into the virtual routing and forwarding (VRF) table on a Cisco ASR 1000 Series Router.

  This condition was observed when reloading a router that was running as a Layer 3 VPN (L3VPN) Provider Edge (PE). This condition occurs because VPNv4 routes may not be imported into the VRF table during the first import scan, which occurs one minute after the BGP session up event.

  There are no known workarounds.

- CSCsv06503

  IPv6 Nonstop Forwarding (NSF) convergence notification may occur before the working set of interfaces become active following an active route processor (RP) Stateful Switchover (SSO) failover to the standby RP.

  There are no known workarounds.

- CSCsv06863

  When the Cisco ASR 1000 Series Router is acting as an L2TP Network Server (LNS)/L2TP Access Concentrator (LAC) in a Virtual Private Dialup Network (VPDN) multihop scenario, the outgoing VPDN call is not forwarded.

  Workaround: Use the **vpdn authen-before-forward** command.

- CSCsv09833

  IP packets larger then 1454 bytes with the “don't fragment” bit set in the IP header are not passing through an IPSec tunnel on a Cisco ASR 1000 Series Router when the maximum transmission unit (MTU) configuration of the tunnel interface and underlying physical interface should allow these packets to pass.

  This condition is observed on Cisco ASR 1000 Series Routers running Cisco IOS XE Release 2.1.x and 2.2.x.

  Workaround: Decrease the IP MTU on the tunnel interface to 1454 or less. To avoid fragmentation of large TCP packets in the network, configure “**ip tcp adjust-mss 1434**” on the tunnel interface.

- CSCsv09874

  The route processor (RP) on a Cisco ASR 1000 Series Router reloads when the router is scaled to support 1K virtual routing and forwarding (VRF) entries with 250K VPNv4 bidirectional prefixes.

  This condition is observed in a Multiprotocol Label Switching (MPLS) over Generic Routing Encapsulation (GRE) with VPN configuration.

  There are no known workarounds.

  Further Problem Description: This condition does not occur when the router is configured with 200 prefixes per VRF and 500 VRF entries.

- CSCsv11231

  When IPSec traffic is present on a Cisco ASR 1004 Router and the **issu loadversion rp 0 file harddisk:asr1000rp1-{rpaccess,rpios,rpcontrol}***version* ***.pkg bay 1 force** command is entered in an attempt to upgrade the router software, the router reloads. The upgrade can continue, but the state is lost.

  Workaround: Disable IPSec during the upgrade, or upgrade without using an in-service software upgrade (ISSU).

- CSCsv14986

  The Cisco QuantumFlow Processor (QFP) on a Cisco ASR 1000 Series Router reloads when multiple subscribers (at a rate of 40 calls per second (CPS)) try to log on using the Spirent Avalanche tool. This condition occurs under the following configuration scenario:

  - IP session as aggregator
  - Static IP without MQC
  - L4 Redirect with VRF web logon

  There are no known workarounds.

- CSCsv17521

  The Cisco ASR 1000 Series Router reloads when unconfiguring Border Gateway Protocol (BGP), access lists, and route map configurations.

  There are no known workarounds.

- CSCsv18533

  When running random packets (with invalid L7 data) with Network Address Translation (NAT) and all Application Line Gateway (ALG) enabled on a Cisco ASR 1000 Series Router for over 24 hours, the following Cisco QuantumFlow Processor (QFP) error occurs:

  ```
  error INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0
  ```

  In addition, the ucode core file returns the following backtrace:

  ```
  0x801C93C9:abort(0x801c935c) 0x6d  0x801AAFE1:rbuf_ooh_handler(0x801aaf8c) 0x55
  0x800206EC:noop(0x800206ec) 0x0  0x801C7C0F:timer_start(0x801c7ba8) 0x67
  0x801A7A3D:chunk_process_retmem_timer(0x801a7924) 0x119
  0x801C46A8:time_process_timer_ev(0x801c4644) 0x64
  0x801C64A8:process_recycle_control(0x801c6414) 0x94
  0x801C8218:mpass_restart_processing(0x801c7f14) 0x304  0x801C88B1:main(0x801c8858)
  0x59  0x80020055:_stext(0x80020000) 0x55  0x80000000:_ResetVector(0x80000000) 0x0
  ```

  There are no known workarounds.

- CSCsv21712

  Input errors were observed on a Cisco ASR 1000 Series Router GE port link to a switch port on a Cisco 7600 Series Router.

  There are no known workarounds.

- CSCsv21861

  When applying Quality of Service (QoS) to a Frame Relay subinterface/PVC on a Cisco ASR 1000 Series Router, the following error message is observed:

  ```
  CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp:  cpp_cp encountered an error1
  ```

  There are no known workarounds.

- CSCsv22428

  On a Cisco ASR 1000 Series Router with Multilink PPP (MLP) configured, a reload of the Embedded Services Processor (ESP) results in the protocol down state on the MLP bundle.

  This condition occurs when Quality of Service (QoS) is configured on the bundle.

  There are no known workarounds.

- CSCsv22769

  In a dual IOS system operating in Route Processor Redundancy (RPR) mode on a Cisco ASR 1000 Series Router, the system unexpectedly reloads on switchover.

  There are no known workarounds.

Resolved Caveats—Cisco IOS XE Release 2.2.2

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.2.2.

- CSCsl08954

  When a SPA on a Cisco ASR 1000 Series Router is shut down with power-on and then enabled again using a powered shutdown as follows

  ```
  hw-module subslot x/y shutdown powered
  no hw-module shutdown
  ```

  ingress packets may be dropped by the forwarding engine under certain conditions, and an intelligent SPA may not come up due to IPC errors.

  Workaround: Use an unpowered shutdown instead: **hw-module subslot x/y shutdown unpowered**.

- CSCsr22845

  Packets generated by the local route processor (RP) on a Cisco ASR 1000 Series Router that are larger than the outgoing interface's maximum transmission unit (MTU) may be dropped after the initial 15 packets.

  This condition occurs when Virtual Fragmentation and Reassembly (VFR) is enabled by the **ip virtual-reassembly** command or features such as Network Address Translation (NAT) are configured on the outgoing interface and packets are locally generated by the RP.

  Workaround: Disable VFR on the outgoing interface using the **no ip virtual-reassembly** command.

- CSCsr36498

  When the **bandwidth** command is applied to any Layer 3 and above physical interface on a Cisco ASR 1000 Series Router, the actual throughput of the physical interface gets changed.

  There are no known workarounds.

- CSCsr41741

  Changing a QoS Model D.2 policy with another QOS Model D.2 policy for 16K IP subscribers using a Change of Authorization (CoA) can cause an Embedded Services Processor (ESP) reload on the Cisco ASR 1000 Series Router.

  This condition occurs because both parent policies have the same child policy name in common. This condition is more apt to occur when scaling up to a large number of sessions such as 16K.

  Workaround: Use different child policy names when pushing a new parent policy through a CoA. The child policies can have the same content.

- CSCsr51820

  Traffic is not forwarded across an IPSec-protected Generic Routing Encapsulation (GRE) tunnel on a Cisco ASR 1000 Series Router when that tunnel is a member of a virtual routing and forwarding (VRF) instance.

  This condition occurs when internal traffic is sourced from or destined to a VRF, and tunnel protection is applied on a tunnel interface whose IP address is a member of that VRF but the source and destination of the tunnel endpoints are in the global routing table.

  There are no known workarounds with tunnel-protection enabled.

- CSCsr51882

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router resets when a service policy is removed from the VIF and CTunnel interfaces.

  Workaround: Disable quality of service (QoS) commands on the VIF and CTunnel interfaces. QoS is not supported on these interfaces.

- CSCsr52410

  A Cisco ASR 1000 Series Router may experience more than 100 millisecond turnaround times (TATs) or message response latencies for H.248 Session/Border Controller (SBC) requests.

  This condition occurs when more than 1000 VLANs are configured. Quality of Service (QoS) statistics collection will also contribute to extended message response latency times.

  Workaround: Reduce the number of configured VLANs and turn off QoS statistics.

- CSCsr58520

  When very large numbers of interfaces are present on the same SIP on a Cisco ASR 1000 Series Router and the SIP is removed from the router, the route processor (RP) reloads with a watchdog error.

  This condition occur under the following scenario:

  - 4000 PPP over Ethernet (PPPoE) sessions over 4000 port-channels, all of which have IPv4 IPv6 enabled
  - 4000 VLANs enabled for IPv4 CEF, and global multicast routing

  Workaround: This watchdog error can be avoided if the interfaces are reconfigured at a slower rate before the SIP is extracted.

- CSCsr60513

  When a class and shape average are configured for the same class on a Cisco ASR 1000 Series Router, the Weighted Random Early Detection (WRED) counters are not updated after enabling Explicit Congestion Notification (ECN).

  There are no known workarounds.

- CSCsr66075

  A Cisco ASR 1000 Series Router running an FRF.12 configuration returns the following error:

  ```
  Jul 30 14:07:03.736 EST: %SPA_CHOC_DSX-3-HDLC_CTRL_ERR: SIP2/0: SPA 2/0: 5 TX Chnl
  Queue Overflow events on HDLC Controller were encountered
  ```

  In addition to this message, packets are dropped.

  This condition is observed on Frame Relay (FR) interfaces where a large percentage of the traffic being sent is fragmented, but which also experience periods of non-fragmented (priority) traffic.

  Workaround: No workaround is required. The message is an indication that packets have been dropped due to an overrun condition. The router will self recover.

- CSCsr67820

  The standby route processor (RP) on a Cisco ASR 1000 Series Router reloads with the following error:

  ```
  %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
  ```

  This condition occurs after a **shut/no shut** of an interface connected to an L2TP Network Server (LNS).

  There are no known workarounds.

- CSCsr75239

  The Cisco QuantumFlow Processor (QFP) on a Cisco ASR 1004 Router occasionally resets when an IOSd switchover occurs with multicast traffic in Stateful Switchover (SSO) mode.

  This condition does not occur on the Cisco ASR 1006 Router or without multicast traffic.

  There are no known workarounds.

- CSCsr87300

  When an ESP switchover is performed on a Cisco ASR 1000 Series Router, resets may occur during the initialization of the new standby ESP.

  This condition is only observed with broadband configurations when ESP1 is the active ESP before the switchover.

  There are no known workarounds.

- CSCsr91559

  A Cisco ASR 1000 Series Router with a fully loaded configuration of 8K VLANs may, under rare conditions, experience a short duration (under one minute) loss of IPv6 unicast traffic on a session.

  This condition only occurs occasionally, such as once in 24 hours.

  Workaround: Reduce the number of services or reduce the load of the configuration to 4K VLANs.

- CSCsr96652

  When a Cisco 8-Port Gigabit Ethernet SPA (SPA-8X1GE-V2) is stopped or removed on a Cisco ASR 1000 Series Router, and the standby route processor (RP) is rebooted and in the process of booting up, large quantities (about 16000) of the following error message appear on the standby RP console:

  ```
  service-policy VLAN_OUTPUT_POLICY can't be attached without corresponding
  service-fragment policy on appropriate target first
  ```

  The appearance of these error messages cannot be turned off, even with **no logging console** configured, and causes the standby RP boot-up time to triple from its usual 15 to 20 minutes to more than 50 minutes.

  This condition occurs because in a Model 3 QoS configuration, the main interfaces must be attached before the fragment policy on the VLAN subinterfaces can be attached. Stopping or removing the SPA-8X1GE-V2 violates this requirement, resulting in the above error messages.

  There are no known workarounds.

- CSCsr99959

  When sending Dynamic Host Configuration Protocol for IPv4 (DHCPv4) requests from 8K users on a Cisco ASR 1000 Series Router, CPU usage on the route processor (RP) becomes higher than 90 percent, which may result in many retransmissions.

  This condition occurs when the router is functioning as a DHCP relay and Customer Premises Equipment (CPEs) connected to the router request IP address assignment through DHCP.

  There are no known workarounds.

- CSCsr99992

  When sending Dynamic Host Configuration Protocol for IPv6 (DHCPv6) requests from 8K users on a Cisco ASR 1000 Series Router, CPU usage on the route processor (RP) becomes higher than 90 percent, which may result in many retransmissions.

  This condition occurs when the router is functioning as a DHCP relay and Customer Premises Equipment (CPEs) connected to the router request IP address assignment through DHCP.

  There are no known workarounds.

- CSCsq13127

  On a Cisco ASR 1000 Series Router running the Session Border Controller with a large number of add/modify/delete messages, the user may see replies to H.248 messages indicating error condition 500 and/or 510.

  There are no known workarounds.

- CSCsu05743

  When performing an In Service Software Upgrade (ISSU) between any two versions of Cisco IOS XE Release 2.1.0, 2.1.1, and 2.1.2 on a Cisco ASR 1000 Series Router, firewall sessions are not synchronized to the standby ESP after ISSU. As a result, the following error message might be reported by the active ESP (F0 in the example below):

  ```
  Sep 11 02:26:03.407 PDT: %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00  Thread:080 TS:00000
  001589974161890 %FWALL-3-HA_INVALID_MSG_RCVD: invalid version 65539 opcode b -Trac
  eback= 801e9f58 800fd87c 800d9489
  ```

  There are no known workarounds; this condition is benign.

- CSCsu05477

  The standby route processor (RP) console on a Cisco ASR 1000 Series Router, which is disabled by default, may occasionally become enabled upon router boot-up. There is no functional impact on the system due to the standby console being enabled.

  There are no workarounds.

- CSCsu10336

  A truncated core file with TEMP_IN_PROGRESS as part of the filename is created on the Cisco ASR 1000 Series Router when a critical process resets on the Embedded Services Processor (ESP) or RP.

  There are no known workarounds.

- CSCsu13500

  The ESP on a Cisco ASR 1000 Series Router unexpectedly reloads when a NetFlow exporter configuration is removed.

  This condition is observed in scenarios with multiple exporters, at least one of which is v9.

  Workaround: Do not remove NetFlow v9 exporter configurations on running systems.

- CSCsu25738

  When reloading an Ethernet SPA immediately after performing a route processor (RP) switchover on a Cisco ASR 1000 Series Router with a high availability (HA) setup and a redundant RP, the error message "%SYS-3-MGDTIMER: Previous timer has bad forward linkage" is displayed on the console. There is no functional impact due to this error message.

  There are no known workarounds.

- CSCsu27642

  When the route processor (RP) on a Cisco ASR 1000 Series Router performs a high availability (HA) failover, IPv6 unicast traffic loss ranging from 5 to 30 seconds occurs for a small number of destinations. The length of the interruption is dependent on the **ipv6 nd reachable-time** value.

  This condition occurs under the following scenario:

  - The router is forwarding IPv6 packets to a large number of destinations.
  - The router has a very large number (several thousand) of neighbor discovery (ND) cache entries.
  - The router performs HA failover from the primary to the secondary.

  Workaround: Set the **ipv6 nd reachable-time** value to ten minutes or longer.

  Further Problem Description: The traffic interruption is caused by the IPv6 ND refreshing cache entries using Neighbor Unreachability Detection (NUD) during HA failover convergence. If the ND has a very large cache, then the additional load of NUD during the convergence period can cause some cache refreshes to fail, which results in the traffic interruption.

- CSCsu27824

  On a Cisco ASR 1000 Series Router, multicast packet loss of about 10 to 20 seconds may be observed under certain conditions about three minutes after a route processor (RP) switchover.

  This condition occurs when the router has approximately 2000 (S,G) entries, each of which is associated with two outgoing interfaces (OIFs). The loss does not occur across all (S,G) entries in the system, but only a subset, and the router recovers within 10 to 20 seconds.

  Workaround: Configure the ip multicast redundancy nsf holdtime to be 60 seconds.

- CSCsu27878

  The Embedded Services Processor (ESP) of a Cisco ASR 1000 Series Router continually loses about 500 kilobytes of memory every 24 hours.

  There are no known workarounds.

  Further Problem Description: Software automatically runs in the background on an ongoing basis to collect and manage traffic statistics accumulated in the ESP's QuantumFlow Processor. This software fails to recycle a few bytes of its memory after each statistics collection. The failure to recycle memory does not affect the router functionality, including the QFP statistics. Under normal circumstances, the router has plenty of ESP free memory (presently, the largest deployed router configuration leaves around 700 MB of free memory), leaving several years' time before this leak exhausts all ESP free memory.

- CSCsu33792

  When a Cisco ASR 1000 Series Router sends or receives traffic in the STALE state, the IPv6 neighbor state does not change to DELAY, PROBE, and then REACH as expected.

  This condition occurs when a cable is removed from and inserted into the GigabitEthernet interface; this condition does not occur when the interface is **shut/no shut**.

  Workaround: Configure a static **ipv6 neighbor** configuration.

- CSCsu35558

  Performing a Simple Network Management Protocol (SNMP) walk on the CISCO-IETF-NAT-MIB on a Cisco ASR 1000 Series Router may cause an Embedded Services Processor (ESP) reload on both the active and standby ESPs.

  There are no known workarounds.

- CSCsu35829

  On a Cisco ASR 1000 Series Router, the fman_rp process reloads and some PPPoE sessions go down and back up again.

  This condition was observed when executing snmp query, copy image, IOS commands and RP commands with 4000 PPPoE sessions and bi-directional traffic.

  There are no known workarounds.

- CSCsu36903

  The tsc-delay timer on a Cisco ASR 1000 Series Router is 500 milliseconds instead of 2000 milliseconds. The reduction of this timer can result in some calls (in which the SIP BYE is delayed) not being torn down cleanly.

  There are no known workarounds.

- CSCsu36908

  When Quality of Service (QoS) and Multicast are configured on the Cisco ASR 1000 Series Router, a performance drop from 10 to 8 Mpps may be experienced after router boot-up.

  There are no known workarounds.

  Further Problem Description: Router performance will revert back to the expected 10Mpps performance after performing a reload of the Embedded Services Processor (ESP).

- CSCsu38990

  When auditing a non-existent pinhole, the following Session Border Controller (SBC) log message (4E03-0131) can appear on the console:

  ```
  *Aug 23 15:57:12.607 JST: %SBC-3-MSG-4E03-0131-4E3E12-2989: SBC/MG-CTRL: A request
  from a controller to SBC-Media could not be processed (for an unknown reason) and will
  be rejected.
  ```

  This message has the potential to flood the console with logs and reduce SBC performance.

  Workaround: Set the console logging level to be greater than 63 (the current default level) to suppress the message.

- CSCsu41375

  The following **show infrastructure punt** commands are not generating output or their output hangs on a Cisco ASR 1000 Series Router:

  - **show platform hardware cpp active infrastructure punt config cause**
  - **show platform hardware cpp active infrastructure punt statistics type inject-drop**
  - **show platform hardware cpp active infrastructure punt statistics type global-drop**

  This condition occurs when continuous traffic is sent on a 10-port Gigabit Ethernet SPA for an extended interval or when the 10-Gbps Cisco ASR 1000 Series ESP (Cisco ASR1000-ESP10) is oversubscribed.

  There are no known workarounds.

- CSCsu41444

  A watchdog reset occurs in the Punt Service Process of a Cisco ASR 1000 Series Router.

  This condition was observed in a configuration with 400K VPNv4 prefixes over 1K virtual routing and forwarding (VRF) instances without any traffic.

  Workaround: Reduce the number of VRFs and prefixes.

- CSCsu43408

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router continually loses about 500 kilobytes of memory every 24 hours.

  There are no known workarounds.

  Further Problem Description: Software automatically runs in the background on an ongoing basis to collect and manage traffic statistics accumulated in the ESP's QuantumFlow Processor. This software fails to recycle a few bytes of its memory after each statistics collection. The failure to recycle memory does not affect the router functionality, including the QFP statistics. Under normal circumstances, the router has plenty of ESP free memory (presently, the largest deployed router configuration leaves around 700 MB of free memory), leaving several years' time before this leak exhausts all ESP free memory.

- CSCsu44885

  The Cisco ASR 1000 Series Router reloads when the **show ip bgp ipv4/ipv6/vpnv4 ... neighbors** command is executed.

  Workaround: Set the terminal length to 0 and use the command with a specific neighbor's address.

- CSCsu47120

  When the Cisco ASR 1000 Series Router reloads several times, the **show facility-alarm status** command reports a CRITICAL Physical Port Link Down on a Gigabit Ethernet SPA.

  Workaround: Issue the **hw-module reload** command on the SPA to clear the alarm.

- CSCsu48111

  When the CPU usage rate of the Control Plane Process (CPP) on a Cisco ASR 1000 Series Router is high, the input policy-map counter is not incremented.

  This condition occurs under the following scenario:

  - Low flow
  - High PPS rate
  - Continuous traffic for 1 minute or more

  There are no known workarounds.

- CSCsu49327

  When large numbers of virtual interfaces are configured on a SPA on a Cisco ASR 1000 Series Router with multicast enabled, a SPA online insertion and removal (OIR) event can cause some outgoing interfaces in the multicast routes to be duplicated in the forwarding hardware. This condition can cause duplicate multicast packets to be generated.

  This condition only occurs with Release2.2.0; it does not occur with later releases.

  Workaround: To avoid the problem, unconfigure the **ipv6 multicast-routing** command before the OIR, and then reconfigure it after the OIR. Another option is to perform the **clear ipv pim reset** command after the OIR event.

  Further Problem Description: This problem is fixed by CSC sr71397.

- CSCsu59082

  Inserting Border Gateway Protocol (BGP) routes into a virtual routing and forwarding (VRF) instance resets the Cisco ASR 1000 Series Router, even if no MPLS-enabled interfaces present.

  Workaround: Upgrade to a more recent image and issue the **mpls label mode all-vrfs protocol all-afs per-vrf** command to configure one label for each VRF to lessen the load on the control plane. (By default the **per-prefix label allocation** is used, that is, one label for each prefix.)

- CSCsu61385

  On a Cisco ASR 1000 Series Router, Peripheral Interface Manager (PIM) state-refresh messages are not generated with a PIM dense mode configuration. As a result, pruned interfaces time out in the forwarding state.

  Workaround: Use PIM dense mode to support only the extremely low rate data traffic. Use PIM Source Specific Mode (SSM) or Sparse Mode to support high rate traffic.

- CSCsu61454

  During a switchover from the active to the standby route processor (RP) on a Cisco ASR 1000 Series Router, multicast Call Admission Control (CAC) reservations may not be preserved. This condition can result in a new client being added before the existing client can re-join. As a result, an existing client may be rejected.

  Workaround: To prevent this condition, configure a multicast Nonstop Forwarding (NSF) hold time that exceeds the Multicast Listener Discovery (MLD) query interval and response time value by using the following configuration command:

  ip multicast redundancy nsf holdtime *delay*

  (To determine the currently configured MLD query interval and response time values on a given interface, use the **show ipv6 mld interface** command. The default MLD query/response time value is 135 seconds.)

- CSCsu64094

  On a Cisco ASR 1000 Series Router, Frame-Relay data-link connection identifier (DLCI) counters do not increment when more than 80 DLCIs are configured on a Frame Relay interface or subinterface.

  There are no known workarounds.

- CSCsu67138

  On a Cisco ASR 1000 Series Router, the **show ip local pool** command does not display the in use IP addresses when an L2TP Network Server (LNS) is configured with high availability (HA) and the **ip local pool** command is configured. As a result after a switchover, IP addresses are not allocated from the pool. This condition results in duplicate IP address assignments.

  There are no known workarounds.

- CSCsu67864

  After the end user replaces his home gateway (HGW) (the DHCP client) physically on a Cisco ASR 1000 Series Router configured as a Dynamic Host Configuration Protocol (DHCP) relay, the new HGW never receives the DHCP Offer from the router. This condition results in the failure of IPv4 address allocation on the newly replaced HGW.

  Workaround: As a temporary workaround, the router administrator can clear the Address Resolution Protocol (ARP) table.

- CSCsu73720

  A Cisco ASR 1000 Series Router running the Session Border Controller feature in distributed mode may experience a software forced reload at very high call setup rates.

  This condition occurs because the high call setup rate causes significant congestion on the route processor.

  There are no known workarounds.

- CSCsu83876

  The Multicast Routing Information Base (MRIB) and the Multicast Forwarding Information Base (MFIB) are out of synchronization after a route processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsu83925

  The group entry displays incorrectly in the **show ipv6 mroute** command and the Protocol Independent Multicast (PIM) topology table on a Cisco ASR 1000 Series Router. This condition occurs if the value of the entry is checked immediately after sending a Multicast Listener Discovery (MLD) join. If you wait a few seconds, the expected group entry value appears in both the **show ipv6 mroute** command and the PIM topology table.

  Workaround: Wait 3 to 5 seconds before checking the value of the group entry after an MLD join.

- CSCsu92950

  When an In Service Software Upgrade (ISSU) is performed from Cisco IOS XE Release 2.2.0 to Cisco IOS XE Release 2.2.2, the mcast OIF count doubles in the Embedded Services Processor (ESP) and Cisco QuantumFlow Processor (QFP).

  This condition does not occur during a normal route processor (RP) switchover from Cisco IOS XE Release 2.2.0 to Cisco IOS XE Release 2.2.2.

  There are no known workarounds.

- CSCsu96316

  When a port-channel member link is shut down on a Cisco ASR 1000 Series Router, 2 to 3 second packet drops are seen before the traffic switches over to the secondary member link in the port-channel.

  This condition occurs when the port-channel is configured to use VLAN load-balancing with two member links, a large number of VLAN subinterfaces are configured, and the primary member link is shut down with traffic.

  There are no known workarounds.

- CSCsu99065

  Some outgoing interfaces (OIFs) are missing from the FP mlist database on a Cisco ASR 1000 Series Router after a quick sequence of (S,G) join-leave-join operations for the multicast entry.

  There are no known workarounds.

- CSCsv58823

  The Cisco QuantumFlow Processor (QFP) driver process on a Cisco ASR 1000 Series Router causes high CPU usage on the forwarding processor.

  This condition occurs when the Cisco QFP driver does not completely process Ternary Content Addressable Memory (TCAM) parity errors, leading to the high CPU usage. This condition also prevents subsequent TCAM parity errors from being corrected.

  Workaround: To resolve the issue, reset the forwarding processor.

Open Caveats—Cisco IOS XE Release 2.2.1

This section documents possible unexpected behavior by Cisco IOS XE Release 2.2.1.

- CSCsl08954

  When a SPA on a Cisco ASR 1000 Series Router is shut down with power-on and then enabled again using a powered shutdown as follows

  ```
  hw-module subslot x/y shutdown powered
  no hw-module shutdown
  ```

  ingress packets may be dropped by the forwarding engine under certain conditions, and an intelligent SPA may not come up due to IPC errors.

  Workaround: Use an unpowered shutdown instead: **hw-module subslot x/y shutdown unpowered**.

- CSCsm16288

  A parser error on the Cisco ASR 1000 Series Router allows the user to select more than one interface using the **show ipv6 mld groups** command. For example, currently the parser allows a syntax of **show ipv6 mld groups fastethernet fastethernet**.

  There are no known workarounds.

- CSCso09886

  When the **show zone security** and **show zone-pair security** commands are executed on the Cisco ASR 1000 Series Router, the console terminal spews all configured zones and zone-pairs.

  This condition occurs when the number of zones and zone-pairs configured exceeds the terminal length value.

  There are no known workarounds.

- CSCso34979

  When executing the **show sbc global dbe media-stats** command on a Cisco ASR 1006 Router configured for the Integrated Session Border Controller, the "Active Media Flows" output may be incorrect.

  Incorrect output can be generated when the following sequence of events occurs: 1. The media state is down on the forwarding engine. 2. An ESP switchover occurs. 3. The media starts before the configured media timeout occurs. The output generated from this point on may be incorrect because the RP believes that the media is down and does not update the state information.

  There are no known workarounds.

- CSCso80547

  After online insertion and removal (OIR) insertion of a SPA on the Cisco ASR 1000 Series Router, the traffic flowing through other SPAs in the SIP are affected/dropped for a few seconds.

  This condition is observed when four POS OC-48 SPAs are used in a single SIP, line-rate traffic is flowing through the SPAs, and one of the OC48 SPAs is OIR removed and inserted into the system.

  There are no known workarounds.

- CSCsq10217

  The following two issues are observed when using route-maps with community lists and the **set ip nexthop** command:

  - With numbered community lists, the community value is not set correctly after the first 100 communities.
  - The next hop is not set correctly after the first ten route-maps. The first ten route maps set the correct next hops. The eleventh route-map sets the same next hop as the tenth route-map and so on. As a result, the **show ip bgp vpnv4** command displays two next hops for these prefixes.

  This condition occurs in a scaled route-map scenario with 101 route-maps that use numbered community lists, or when more than ten route-maps that set the IP next hop.

  There are no known workarounds.

- CSCsq11257

  After the insertion of 1-port channelized STM1/OC3 SPAs (SPA-1XCHSTM1/OC3) into a SIP on the Cisco ASR 1000 Series Router, the **show memory debug leaks** command displays leaks in the IOSd IPC task. The leaks do not increase and remain constant until the SPAs are re-inserted into the SIP. After the SPAs are re-inserted into the SIP, the existing leaks are freed and new leaks are observed.

  There are no known workarounds.

- CSCsq67414

  LineStatusChange traps on the Cisco ASR 1000 Series Router show incorrect indexes when the line status changes.

  This condition occurs when the loopback status changes for the T1 line and traps are generated.

  There are no known workarounds.

- CSCsq69183

  When removing a class from a policy map on the Cisco ASR 1000 Series Router, the remaining percentages of the other user defined classes might not get adjusted if the configuration has a shaper or queue-limit. (If the class has a **bandwidth** command, the percentages do get adjusted.)

This condition affects only some configurations with shaper or queueing in user defined classes; some shaper or queueing configurations function as expected.

There are no known workarounds.

- CSCsq70140

  The following error message appears on the Cisco ASR 1002 Router and the Cisco ASR 1004 Router:

  ```
  No memory available: Update of NVRAM config failed!
  ```

  This message appears more frequently when the user is saving a very big configuration, such as a configuration with 16K interfaces on a Cisco ASR 1002 Router or Cisco ASR 1004 Router. This problem is not seen on the Cisco ASR 1006 Router.

  There are no known workarounds.

- CSCsq73935

  When a 1xCHSTM1/OC3-SPA is configured with Sonet framing/t3 mode an invalid instance of “0” is getting populated for tabular objects in the dsx3ConfigTable.

  Workaround: If the mode is set to “ct3” or “ct3-e1”, the “0” instances are not returned.

- CSCsq76871

  Under certain circumstances, the Cisco ASR 1000 Series Router drops logging messages from the console while the startup configuration is being parsed.

  This condition occurs because under certain configurations the buffered log output differs from the console output. In these configurations, some logging messages are dropped by the console, but are saved within the buffered log.

  Workaround: Increase the size of the synchronous logging queues by configuring a large enough logging synchronous level 0 limit for the console line so that log messages are no longer dropped from the console during configuration boot.

  For example:

  ```
  line con 0
  logging synchronous level 0 limit 5000
  stopbits 1
  ```

- CSCsq77104

  When you configure Control Plane Policing (CoPP) to police ingress IPv6 echo request (ping) packets or configure CoPP to police egress IPv6 echo response (ping response) packets on a Cisco ASR 1000 Series Router, neither of these packet types are matched to the appropriate class-map or policed according to the configured service-policy. Instead, these packets are classified as the class-default.

  Workaround: Configure policing of ingress IPv6 Internet Control Message Protocol (ICMP) echo request packets or egress IPv6 ICMP echo response packets at the interface level.

- CSCsq78536

  When you attempt to quit or escape the **show policy-map session output** command on the Cisco ASR 1000 Series Router, the command takes a long time to terminate when a large number of PPP over Ethernet (PPPoE) sessions exist.

  This condition occurs when there is hierarchical queueing involved. The delay increases in proportion to the number of sessions present.

  There are no known workarounds. The only option is to wait approximately 90 seconds until the command terminates.

- CSCsq83554

  The LinkDown trap is generated twice for a T1 line when the **shutdown** command is issued for the Sonet controller on a 1xCHSTM-OC3 SPA on the Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsq91659

  When a 1xCHSTM-OC3 SPA on the Cisco ASR 1000 Series Router is configured in unframed E1 mode and the SPA is reloaded using the **hw-module** *subslot* **reload** command, dsx1LineStatus returns an invalid value of "0."

  There are no known workarounds.

- CSCsq93212

  Upon reload of a Cisco ASR 1000 Series Router, the standby RP may see a feature installation error on an L2TP Network Server (LNS) session when Model D.2 QoS is configured.

  There are no workarounds; the session must be re-established to download the feature.

- CSCsr10631

  On a Cisco ASR 1000 Series Router with a highly-scaled PPP Termination Aggregation (PTA) configuration and QoS applied, the call per setup (CPS) rate drops to 35 calls established per second.

  This condition occurs when PTA is configured on a large numbers of sessions (16K sessions), QoS is applied to the sessions, and all sessions are brought up simultaneously.

  There are no known workarounds.

- CSCsr10774

  When the **clear ip subscriber** command is issued on the Cisco ASR 1000 Series Router, it can take up to 10 minutes to clear 16K subscriber sessions. Although the **show subscriber statistics** command indicates the sessions are gone, the **show platform hardware qfp active feature ess session | include Current** command indicates the sessions are still present. In addition, tracebacks (such as, cpp_ess_ea_ipsub_l2_remove_hash_elem) appear during the teardown process.

  This infrequent condition occurs if the sessions have QoS configured when the **clear ip subscriber** command is issued.

  Workaround: Distribute the subscriber sessions across multiple interfaces (for example, 4K subscribers per interface) so that the impact of one interface shutdown does not generate a complete loss of all sessions in the system.

- CSCsr18279

  In rare conditions when bidirectional forwarding detection (BFD) is shut down on the Cisco ASR 1000 Series Router, a harmless traceback error message is printed.

  There are no known workarounds.

- CSCsr22845

  Packets generated by the local RP on a Cisco ASR 1000 Series Router that are larger than the outgoing interface's maximum transmission unit (MTU) may be dropped after the initial 15 packets.

  This condition occurs when Virtual Fragmentation and Reassembly (VFR) is enabled by the **ip virtual-reassembly** command or features such as Network Address Translation (NAT) are configured on the outgoing interface and packets are locally generated by the RP.

  Workaround: Disable VFR on the outgoing interface using the **no ip virtual-reassembly** command.

- CSCsr24160

  A large scale configuration on a Cisco ASR 1000 Series Router with 1000 routes and 500 clients, reports lower than expected Border Gateway Protocol (BGP) route reflection performance. The routing convergence is about 25% slower than expected.

  There are no known workarounds.

- CSCsr27155

  After an RP switchover on a Cisco ASR 1000 Series Router under traffic load, the following traceback may be seen at the new standby RP:

  ```
  ASR1000_RP_DPIDB-3-IDXLOOKUPFAILED
  ```

  This condition may occur in a scaled configuration (such as 16K sessions/1 tunnel established with a Model D.2 QoS configuration terminated at an L2TP Access Concentrator (LAC)), when an RP switchover is performed.

  There are no known workarounds.

- CSCsr41741

  Changing a QoS Model D.2 policy with another QOS Model D.2 policy for 16K IP subscribers using a Change of Authorization (CoA) can cause an Embedded Services Processor (ESP) reload on the Cisco ASR 1000 Series Router.

  This condition occurs because both parent policies have the same child policy name in common. This condition is more apt to occur when scaling up to a large number of sessions such as 16K.

  Workaround: Use different child policy names when pushing a new parent policy through a CoA. The child policies can have the same content.

- CSCsr43311

  The Cisco QuantumFlow Processor (QFP) on the Cisco ASR 1000 Series Router encounters an exception when encapsulation is configured on an asynchronous interface.

  There are no known workarounds.

- CSCsr45682

  Initiating 12K broadband L2TP Access Concentrator (LAC) sessions with QoS configured on a Cisco ASR 1000 Series Router may result in Embedded Services Processor (ESP) software tracebacks.

  This condition may impact desirable QoS behaviors.

  There are no known workarounds.

- CSCsr46529

  Deleting and then adding an interface configuration on a Multilink PPP (MLP) bundle with IPSec configured may trigger an Embedded Services Processor (ESP) reset on the Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsr50040

  If you disable **aaa policy interface-config allow-subinterface** on the Cisco ASR 1000 Series Router on a subinterface that has RADIUS attributes (such as an lcp:interface-config) creating full virtual access for broadband access (BBA) sessions, the system may report error messages and tracebacks.

  Workaround: Configure **aaa policy interface-config allow-subinterface** locally on the router.

- CSCsr51820

  Traffic is not forwarded across an IPSec-protected Generic Routing Encapsulation (GRE) tunnel on a Cisco ASR 1000 Series Router when that tunnel is a member of a virtual routing and forwarding (VRF) instance.

  This condition occurs when internal traffic is sourced from or destined to a VRF, and tunnel protection is applied on a tunnel interface whose IP address is a member of that VRF but the source and destination of the tunnel endpoints are in the global routing table.

  There are no known workarounds with tunnel-protection enabled.

- CSCsr53729

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reset while performing a software switchover in Stateful Switchover (SSO) mode with IPSec and Multilink PPP (MLPPP) configured.

  This condition has been observed on a Cisco ASR 1004 Router.

  There are no known workarounds.

- CSCsr55626

  A Cisco ASR 1000 Series Router allows you to apply DRL to a session that already has QoS applied. DRL and QoS should be mutually exclusive.

  This condition does not occur when DRL is applied first and then QoS is applied.

  There are no known workarounds.

- CSCsr56358

  When an RP switchover is performed on the Cisco ASR 1000 Series Router under traffic load, some sessions at the new standby RP have the SSM remote session ID set to 0.

  This condition occurs in scaled configurations (for example, 16K sessions/1 tunnel established with Model D.2 QoS configuration terminated at an L2TP Access Concentrator (LAC)).

  There are no known workarounds.

- CSCsr59527

  When buffers are unconfigured on the Cisco ASR 1000 Series Router, tracebacks are generated. These tracebacks have no functional impact on the operation of the system.

  There are no known workarounds.

- CSCsr68177

  Disabling and enabling the Cisco Discovery Protocol (CDP) on the Cisco ASR 1000 Series Router causes an interface associated with virtual routing and forwarding (VRF) instances to flap.

  Workaround: Remove VRF configurations from the interface.

- CSCsr72171

  When the Cisco QuantumFlow Processor (QFP) on a Cisco ASR 1000 Series Router is reloaded with a scaled Point-to-Point Protocol (PPP) broadband session configuration, traceback messages from the Cisco QFP are displayed on the IOS console.

  This condition was observed when the Cisco QFP was reloaded using the **hw-module slot reload** command with a 16K sessions/8K tunnels configuration.

  There are no known workarounds.

- CSCsr75239

  The Cisco QuantumFlow Processor (QFP) on a Cisco ASR 1004 Router occasionally resets when an IOSd switchover occurs with multicast traffic in Stateful Switchover (SSO) mode.

  This condition does not occur on the Cisco ASR 1006 Router or without multicast traffic.

  There are no known workarounds.

- CSCsr76562

  An unexpected StopCCN is retransmitted on a Cisco ASR 1000 Series Router after a StopCCN has already been sent.

  This condition occurs when the router is functioning as an L2TP access concentrator (LAC) and no L2TP network server (LNS) exists.

  There are no known workarounds.

- CSCsr81066

  When a Cisco ASR 1000 Series Router is configured with more than 140 PVCs and a packet size above 1490, Frame Relay PVC statistics are not updated properly.

  There are no known workarounds.

- CSCsr85028

  Under rare conditions, when performing a **write mem** on the active RP of a Cisco ASR 1000 Series Router, the standby RP fails to synchronize the configuration from the active RP and is forced to reload. After the forced reload, the standby RP comes up, achieves SSO, and operates as expected.

  There are no known workarounds.

- CSCsr85690

  The following traceback appears after a hardware reload of a GigaEthernet (GE) SPA on a Cisco ASR 1000 Series Router:

  ```
  Aug 8 14:45:33 MCP1: %ASR1000_INFRA-5-IOS_INTR_OVER_LIMIT: IOS thread disabled
  interrupt for 15 msec
  ```

  This condition occurs on a router configured with 4K Layer 2 Tunnel Protocol (L2TP) sessions and tunnels with shape QoS policies applied to each session.

  There are no known workarounds.

- CSCsr85737

  Consecutive execution of the **hw-module subslot** *x*/*y* command after a SPA reload on a Cisco ASR 1000 Series Router results in the following message:

  ```
  %Command cannot be executed. Standby initialization in progress
  ```

  There are no known workarounds.

- CSCsr87974

  When the online insertion and removal (OIR) of a SIP is performed on a Cisco ASR 1000 Series Router, traceback occurs at fibidb_configure_lc_ipfib. No functional impact is observed.

  There are no known workarounds.

- CSCsr88298

  Multiple tracebacks appear at get_free_event_q_elt when initiating a PPP over X (PPPoX) session with Per-Subscriber Firewall enabled on a Cisco ASR 1000 Series Router. No functional impact is observed.

This condition occurs when the zone-member configuration has been downloaded from a RADIUS server.

Workaround: Use a local zone-member configuration instead of a RADIUS download for Per-Subscriber Firewall.

- CSCsr89529

  Heartbeat failures are detected on channelized SPAs on the Cisco ASR 1000 Series Router.

  Workaround: Reload the SPA.

- CSCsr90264

  When RADIUS authentication is used and an identical zone statement is downloaded from RADIUS as an existing zone statement in the virtual-template, subscriber call attempts fail. The router logs include the following message:

  Zoning is currently not configured for interface Virtual-Access

  Workaround: Ensure that when the **aaa policy interface-config allow-subinterface** statement is configured for the virtual-template, the analogous **lcp:interface-config=allow-subinterface=yes** statement is either not configured by RADIUS or uses a different zone name.

- CSCsr91559

  A Cisco ASR 1000 Series Router with a fully loaded configuration of 8K VLANs may, under rare conditions, experience a short duration (under one minute) loss of IPv6 unicast traffic on a session.

  This condition only occurs occasionally, such as once in 24 hours.

  Workaround: Reduce the number of services or reduce the load of the configuration to 4K VLANs.

- CSCsr92450

  Unconfiguring Frame Relay interfaces on a Cisco ASR 1000 Series Router may lead to an Embedded Services Processor (ESP) software reset.

  This condition occurs when a QoS configuration is applied to the Frame Relay interfaces.

  There are no known workarounds.

- CSCsr92883

  After certain Embedded Services Processor (ESP) switchovers on a Cisco ASR 1000 Series Router, the new standby ESP may generate TIMEHOG messages when the standby has completed booting. The messages are informational and do not affect router operation.

  This condition is generally only observed when the switchover is caused by a physical online insertion and removal (OIR) of the active ESP. It may also happen after other types of switchover.

  There are no known workarounds.

- CSCsr92999

  On a Cisco ASR 1000 Series Router with a lot of interfaces, the Session Border Controller (SBC) H.248 call setup rate may fall when the standby RP is booting up.

  Workaround: Enter the **parser config cache interface** command and the **show running-config** command before bringing up the standby RP.

- CSCsr94074

  A Gigabit Ethernet SPA interface on a Cisco ASR 1000 Series Router with a 100M FX SFP may not ping after a **shut/no shut**, online insertion and removal (OIR), or power cycle.

  This condition may cause the interface to drop traffic.

Workaround: Issue another **shut/no shut** on the SPA to clear the condition. Note that if there is enough delay (around 10 seconds) between successive shuts and no shuts, the condition is less likely to occur.

- CSCsr95924

  When an SNMP trap for the CEF peer-fib-state-change is enabled after multiple RP switchovers on a Cisco ASR 1000 Series Router the following traceback message may appear at the console:

  ```
  Aug 14 11:11:33.037: %SYS-3-CPUHOG: Task is running for (2023)msecs, more than
  (2000)msecs (12/12),process = IPC LC Message Handler.
  ```

  This condition occurs with a Multiprotocol Label Switching (MPLS) Layer 3 VPN (L3VPN) configuration that consists of large numbers of VPNs and Border Gateway Protocol (BGP) peers.

  The traceback has no functional impact.

  Workaround: Disable the SNMP trap for the CEF peer-fib-state-change by removing the following line from the configuration: **snmp-server enable traps cef peer-fib-state-change**.

- CSCsr95653

  A Cisco ASR 1000 Series Router may experience more than 100ms turnaround times (TATs) or message response latencies for H.248 Session Border Controller (SBC) requests.

  There are no known workarounds.

- CSCsr96219

  A Cisco ASR 1000 Series Router configured with ip virtual-reassembly, ip nat outside, and frame relay fragmentation on an interface/subinterface generates the following error message:

  ```
  %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread:044 TS:00000004308774891044
  %ATTN-3-SYNC_TIMEOUT: msecs since last timeout 4304017, missing packets 1
  ```

  The error message does not necessarily mean a packet is physically missing; it can indicate an internal bug of packet tracking in the system.

  There are no known workarounds.

- CSCsr96652

  When a Cisco 8-Port Gigabit Ethernet SPA (SPA-8X1GE-V2) is stopped or removed on a Cisco ASR 1000 Series Router, and the standby RP is rebooted and in the process of booting up, large quantities (about 16000) of the following error message appear on the standby RP console:

  ```
  service-policy VLAN_OUTPUT_POLICY can't be attached without corresponding
  service-fragment policy on appropriate target first
  ```

  The appearance of these error messages cannot be turned off, even with **no logging console** configured, and causes the standby RP boot up time to triple from its usual 15 to 20 minutes to more than 50 minutes.

  This condition occurs because in a Model 3 QoS configuration, the main interfaces must be attached before the fragment policy on the VLAN subinterfaces can be attached. Stopping or removing the SPA-8X1GE-V2 violates this requirement, resulting in the above error messages.

  There are no known workarounds.

- CSCsr97059

  When a Flexible Packet Matching (FPM) class is replaced with a similar class within the same parent policy on a Cisco ASR 1000 Series Router, the correct FPM action is not followed. Packets are still being allowed through the router; the expected action would be for packets to be dropped due to the drop action child policy.

The **show policy-map type access-control interface** output shows the FPM classification as correct.

Workaround: If you re-add the original class, the correct FPM action is followed.

- CSCsr97633

  External BGP (eBGP) neighbors on a Cisco ASR 1000 Series Router get stuck in the OpenSent state after an RP switchover until the hold-time expires.

  This condition causes traffic drop.

  There are no known workarounds.

- CSCsu05477

  The standby RP console on a Cisco ASR 1000 Series Router, which is disabled by default, may occasionally become enabled upon router boot-up. There is no functional impact on the system due to the standby console being enabled.

  There are no workarounds.

- CSCsu06783

  When using a scaled Policy Based Routing (PBR) configuration with a large number of subinterfaces and Border Gateway Protocol (BG)P sessions on a Cisco ASR 1000 Series Router, the BGP sessions go down.

  This condition is observed under the following scenario:

  – When a large PBR configuration (of several hundred route-maps) is used with a large number (several hundred) of subinterfaces.

  – When the IP virtual routing and forwarding (VRF) selection feature is also configured on the subinterfaces and route-map.

  – When a large number (several hundred) of BGP sessions are in use.

  There are no known workarounds.

- CSCsu10336

  A truncated core file with TEMP_IN_PROGRESS as part of the filename is created on the Cisco ASR 1000 Series Router when a critical process resets on the Embedded Services Processor (ESP) or RP.

  There are no known workarounds.

- CSCsu10406

  The following error message is generated when reloading the Embedded Services Processor (ESP) on a Cisco ASR 1004 Router with IPSec configured on the chassis:

  ```
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp: cpp_cp encountered an error1
  ```

  The IPSec tunnels come up as normal.

  There are no known workarounds.

- CSCsu18185

  When traffic classification (TC) is applied to a subscriber session on a Cisco ASR 1000 Series Router using an undefined access control list (ACL), the packet counters are not updated for Intelligent Services Gateway (ISG).

  Workaround: Define the ACLs explicitly instead of using an undefined ACL.

- CSCsu25738

  When reloading an Ethernet SPA immediately after performing an RP switchover on a Cisco ASR 1000 Series Router with a high availability (HA) setup and a redundant RP, the error message "%SYS-3-MGDTIMER: Previous timer has bad forward linkage" is displayed on the console. There is no functional impact due to this error message.

  There are no known workarounds.

- CSCsu27642

  When the RP on a Cisco ASR 1000 Series Router performs a high availability (HA) failover, IPv6 unicast traffic loss ranging from 5 to 30 seconds occurs for a small number of destinations. The length of the interruption is dependent on the **ipv6 nd reachable-time** value.

  This condition occurs under the following scenario:

  - The router is forwarding IPv6 packets to a large number of destinations.
  - The router has a very large number (several thousand) of neighbor discovery (ND) cache entries.
  - The router performs HA failover from the primary to the secondary.

  Workaround: Set the **ipv6 nd reachable-time** value to ten minutes or longer.

  Further Problem Description: The traffic interruption is caused by the IPv6 ND refreshing cache entries using Neighbor Unreachability Detection (NUD) during HA failover convergence. If the ND has a very large cache then the additional load of NUD during the convergence period can cause some cache refreshes to fail, which results in the traffic interruption.

- CSCsu27824

  On a Cisco ASR 1000 Series Router, multicast packet loss of about 10 to 20 seconds may be observed under certain conditions about three minutes after an RP switchover.

  This condition occurs when the router has approximately 2000 (S,G) entries, each of which is associated with two outgoing interfaces (OIFs). The loss does not occur across all (S,G) entries in the system, but only a subset, and the router recovers within 10 to 20 seconds.

  Workaround: Configure the ip multicast redundancy nsf holdtime to be 60 seconds.

- CSCsu27878

  The Embedded Services Processor (ESP) of a Cisco ASR 1000 Series Router continually loses roughly 500 kilobytes of memory every 24 hours.

  There are no known workarounds.

  Further Problem Description: Software automatically runs in the background on an ongoing basis to collect and manage traffic statistics accumulated in the ESP's QuantumFlow Processor. This software fails to recycle a few bytes of its memory after each statistics collection. The failure to recycle memory does not affect the router functionality, including the QFP statistics. Under normal circumstances, the router has plenty of ESP free memory (presently, the largest deployed router configuration leaves around 700 MB of free memory), leaving several years' time before this leak exhausts all ESP free memory.

- CSCsu29303

  The following error message is observed on a Cisco ASR 1000 Series Router with a large configuration and PPP over Ethernet (PPPoE) configured:

  ```
  %EVENTLIB-3-TIMEHOG: F1: cpp_cp: undefined: 69405ms, Traceback= .....
  ```

  This message has no adverse impact on router functionality.

  There are no known workarounds.

- CSCsu33792

  When a Cisco ASR 1000 Series Router sends or receives traffic in the STALE state, the IPv6 neighbor state does not change to DELAY, PROBE, and then REACH as expected.

  This condition occurs when a cable is removed from and inserted into the GigabitEthernet interface; this condition does not occur when the interface is **shut/no shut**.

  Workaround: Configure a static **ipv6 neighbor** configuration.

- CSCsu35558

  Performing an SNMP walk on the CISCO-IETF-NAT-MIB on a Cisco ASR 1000 Series Router may cause an Embedded Services Processor (ESP) reload on both the active and standby ESPs.

  There are no known workarounds.

- CSCsu35640

  The RP on a Cisco ASR 1000 Series Router resets with following traceback when the **ip pim send-rp-discovery** command is unconfigured in global configuration mode:

  ```
  ASR1000-WATCHDOG: Process = Exec
  ```

  This condition occurs when the router is configured for PPP Terminated Aggregation (PTA) and per session multicast traffic, and 4K or 8K PPP over Ethernet (PPPoE) sessions are up.

  Workaround: Do not unconfigure the **ip pim send-rp-discovery** command in global configuration mode when 4K or 8K PPPoE sessions are up.

- CSCsu39895

  The IOSd process resets on the active RP on a Cisco ASR 1000 Series Router when the RP is running IPv4/6 unicast and IPv6 multicast traffic. The following error message is observed in the crashinfo file:

  ```
  000219: Sep 2 04:21:58.350 EDT: %SYS-2-MALLOCFAIL: Memory allocation of 1128 bytes
  failed from 0x124D2F64, alignment 0
  Pool: Processor Free: 449920 Cause: Memory fragmentation
  Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "ASR1000-RP Punt
  Service Process", ipl= 0, pid= 71
  -Traceback= 1#106b90f504fce8544ce4979667ec2d5d :10000000+50BF84 :10000000+50A19C
  :10000000+50A46C :10000000+15399A4 :10000000+153F834 :10000000+153FE34
  :10000000+24D2F68 :10000000+24D371C :10000000+24D3FC4 :10000000+24D21DC
  :10000000+8DF4B0 :10000000+8DFDB4 :10000000+8E022C :10000000+8E0298 :10000000+8D6030
  :10000000+265E11C
  ```

  There are no known workarounds.

- CSCsu41375

  The following **show infrastructure punt** commands are not generating output or their output hangs on a Cisco ASR 1000 Series Router:

  - **show platform hardware cpp active infrastructure punt config cause**
  - **show platform hardware cpp active infrastructure punt statistics type inject-drop**
  - **show platform hardware cpp active infrastructure punt statistics type global-drop**

  This condition occurs when continuous traffic is sent on a 10-port Gigabit Ethernet SPA for an extended interval or when the 10-Gbps Cisco ASR 1000 Series ESP (ASR1000-ESP10) is oversubscribed.

  There are no known workarounds.

- CSCsu41444

  A watchdog reset occurs in the Punt Service Process of a Cisco ASR 1000 Series Router.

  This condition was observed in a configuration with 400K VPNv4 prefixes over 1K virtual routing and forwarding (VRF) instances without any traffic.

  Workaround: Reduce the number of VRFs and prefixes.

- CSCsu42105

  The Cisco ASR 1000 Series Router does not re-mark the differentiated services code point (DSCP) for the following IPv6 neighbor discovery (ND) packets:

  – The Duplicate Address Detection (DAD) neighbor solicitation (NS) packet for the link local address

  – The neighbor advertisement (NA) (Frame 55) for the link local address after a link flap

  There are no known workarounds.

- CSCsu43290

  On a Cisco ASR 1000 Series Router, performing a start/stop of two SPAs at the same time with triple play traffic may cause the following traceback to appear at the console:

  ```
  %SYS-2-NOTQ: unqueue didn't find 3B8B8D64 in queue 1407A5C0 -Process= "
  CHKPT rcv MSG process", ipl= 2, pid= 80
  ```

  There is no functional impact due to this traceback.

  There are no known workarounds.

- CSCsu43408

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router continually loses roughly 500 kilobytes of memory every 24 hours.

  There are no known workarounds.

  Further Problem Description: Software automatically runs in the background on an ongoing basis to collect and manage traffic statistics accumulated in the ESP's QuantumFlow Processor. This software fails to recycle a few bytes of its memory after each statistics collection. The failure to recycle memory does not affect the router functionality, including the QFP statistics. Under normal circumstances, the router has plenty of ESP free memory (presently, the largest deployed router configuration leaves around 700 MB of free memory), leaving several years' time before this leak exhausts all ESP free memory.

- CSCsu44557

  On a Cisco ASR 1000 Series Router, the memory allocation for Border Gateway Protocol (BGP) processes on the RP increases after clearing BGP sessions. In addition, the BGP summary counter is also incorrectly incremented.

  There are no known workarounds.

- CSCsu45138

  On a Cisco ASR 1000 Series Router, the Service Control Engine (SCE) sends the wrong IP address in a session query request to the Intelligent Services Gateway (ISG).

  There are no known workarounds.

- CSCsu45307

  The number of sessions in the READY state on the standby RP of a Cisco ASR 1000 Series Router does not match the number of sessions in the READY state on the currently active RP.

  This condition occurs with 16K active sessions when both the Point-to-Point Protocol (PPP) and QoS are configured. If just PPP is configured, the problem does not occur.

  There are no known workarounds.

- CSCsu46027

  When a port-channel member link failure and an RP failover occur in close proximity, the Cisco ASR 1000 Series Router does not switch outgoing traffic from the failed member link to the secondary member link immediately. This condition can occasionally result in packet loss of more than 10 seconds for packets that used to be active on the failed link.

  This condition is observed on a router with 8000 VLAN subinterfaces across 8 port channels under the following scenario:

  - Each port channel has 1000 VLAN subinterfaces.
  - Each port-channel interface consists of two physical Gigabit Ethernet interfaces from two different SPAs.
  - Manual VLAN load-balancing is configured in which 500 VLAN subinterfaces are active on each of the member links and the other member link is the standby.

  There are no known workarounds.

- CSCsu46531

  On a Cisco ASR 1000 Series Router, the active RP CPU utilization spikes for 40 seconds, as the active RP works through the process of synchronizing a large customer configuration to the standby RP.

  There are no known workarounds.

- CSCsu47120

  When the Cisco ASR 1000 Series Router reloads several times, the **show facility-alarm status** command reports a CRITICAL Physical Port Link Down on a Gigabit Ethernet SPA.

  Workaround: Issue the **hw-module reload** command on the SPA to clear the alarm.

- CSCsu47716

  Point-to-Point Protocol (PPP) session disconnects occur on a Cisco ASR 1000 Series Router because of Link Control Protocol (LCP) negotiation failures. The sessions eventually do come up.

  There are no known workarounds.

- CSCsu48111

  When the CPU usage rate of the Cisco QuantumFlow Processor (QFP) on a Cisco ASR 1000 Series Router is high, the input policy-map counter is not incremented.

  This condition occurs under the following scenario:

  - Low flow
  - High PPS rate
  - Continuous traffic for 1 minute or more

  There are no known workarounds.

- CSCsu48364

  A QoS configuration does not get successfully installed in the Cisco QuantumFlow Processor (QFP) after an RP switchover on a Cisco ASR 1000 Series Router. Tracebacks of the following form are observed on the IOS console:

  ```
  FMFP-3-OBJ_DWNLD_TO_CPP_FAILED
  ```

  This condition occurs in scaled scenarios such as 16K sessions/8K tunnels with a Model D.2 QoS configuration.

  There are no known workarounds.

- CSCsu50406

  When a Cisco ASR 1000 Series Router is reloaded or an online insertion and removal (OIR) insertion is performed on one of its SPAs, an error message is generated and the QoS policy is suspended.

  This condition occurs when a QoS policy is attached to the Multilink PPP (MLP) bundle that has **shape %** *n* configured where *n* is less than 13.

  Workaround: Manually remove and then reattach the QoS policy to the MLP bundle.

- CSCsu50921

  When more than 500 IPSec sessions are brought up, cleared and then brought up again across a Dynamic Virtual Tunnel Interface (DVTI) and Easy VPN (EzVPN) setup on a Cisco ASR 1000 Series Router, the IPSec tunnels come up but traffic doesn't get through and Cisco QuantumFlow Processor (QFP) flows cease to exist.

  Workaround: Use dynamic crypto maps with EzVPN instead of Dynamic VTI.

- CSCsu53066

  A Cisco ASR 1000 Series Router may experience more than 100 millisecond turnaround times (TAT) or message response latencies for H.248 Session Border Controller (SBC) requests.

  QoS statistics collection and regular changes in the VLAN configuration can also contribute to the extended message response latencies.

  Workaround: Reduce the number of configured VLANs, turn off QoS statistics, and minimize the amount of VLAN configuration changes to help keep the message response latencies down. Message response latencies can also be minimized by issuing the **parser config cache interface** command and the **show running-config** command prior to allowing H.248 SBC requests into the system.

- CSCsu55070

  If **no cdp enable** is configured on a few ports on a POS-OC48 SPA and the Cisco ASR 1000 Series Router is reloaded, the Cisco Discovery Protocol (CDP) gets disabled on all the ports.

  This condition occurs when the configuration is saved prior to the reload.

  Workaround: Add **cdp enable** to the ports you do not want to have disabled prior to the reload.

- CSCsu59082

  Inserting Border Gateway Protocol (BGP) routes into a virtual routing and forwarding (VRF) instance resets the Cisco ASR 1000 Series Router, even if no MPLS-enabled interfaces present.

  Workaround: Upgrade to a more recent image and issue the **mpls label mode all-vrfs protocol all-afs per-vrf** command to configure one label for each VRF to lessen the load on the control plane. (By default the **per-prefix label allocation** is used, that is, one label for each prefix.)

- CSCsu61385

  On a Cisco ASR 1000 Series Router, Peripheral Interface Manager (PIM) state-refresh messages are not generated with a PIM dense mode configuration. As a result, pruned interfaces time out in the forwarding state.

  Workaround: Use PIM dense mode to support only the extremely low rate data traffic. Use PIM Source Specific Mode (SSM) or Sparse Mode to support high rate traffic.

- CSCsu64094

  On a Cisco ASR 1000 Series Router, Frame-Relay data-link connection identifier (DLCI) counters do not increment when more than 80 DLCIs are configured on a Frame Relay interface or subinterface.

  There are no known workarounds.

- CSCsu67138

  On a Cisco ASR 1000 Series Router, the **show ip local pool** command does not display the in use IP addresses when an L2TP Network Server (LNS) is configured with high availability (HA) and the **ip local pool** command is configured. As a result after a switchover, IP addresses are not allocated from the pool. This condition results in duplicate IP address assignments.

  There are no known workarounds.

- CSCsu67864

  After the end user replaces his home gateway (HGW) (the DHCP client) physically on a Cisco ASR 1000 Series Router configured as a Dynamic Host Configuration Protocol (DHCP) relay, the new HGW never receives the DHCP Offer from the router. This condition results in the failure of IPv4 address allocation on the newly replaced HGW.

  Workaround: As a temporary workaround, the router administrator can clear the Address Resolution Protocol (ARP) table.

- CSCsu91220

  The **show issu version detail** command fails on a Cisco ASR 1000 Series Router with the error "Error connecting to command relay server".

  This problem is observed when the **no ip subnet-zero** command is configured in the system startup configuration.

  Workaround: Remove the **no ip subnet-zero** configuration command from the startup configuration and reload the system.

Resolved Caveats—Cisco IOS XE Release 2.2.1

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.2.1.

- CSCsm27071

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload. Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml