Release 2.1 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 2.1.2

This section documents possible unexpected behavior by Cisco IOS XE Release 2.1.2

- CSCsm55507

  On a Cisco ASR 1000 Series Router, when the IP MTU on a Generic Routing Encapsulation (GRE) tunnel interface exceeds that on the physical interface carrying tunnel traffic, the traffic requiring fragmentation may be dropped over time.

  Workaround: Configure an IP MTU on the tunnel interface no greater than that on the physical interface carrying tunnel traffic.

- 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, and various control plane functions such as Session Border Controller (SBC) call setup may not function as expected.

  Workaround: Reduce the **show run** command output to a file for post-processing.

- CSCsq08067

  On a Cisco ASR 1000 Series Router, if the **nbar protocol-discovery** command is configured on multiple interfaces (for example, 200) using the **interface range** command, then the **nbar protocol-discovery** configuration is removed from all VLANs except the first VLAN after an RP switchover.

  This condition occurs after an RP switchover on the Cisco ASR 1006 Router, or an IOSd switchover on the Cisco ASR 1004 Router.

  Workaround: Instead of using the **interface range** command, configure the **nbar protocol-discovery** command for each interface individually.

- CSCsq22332

  After provisioning different name servers in the global IP view and within a VRF on a Cisco ASR 1000 Series Router, a ping to a host within the VRF uses the name server in the global space to attempt to resolve the hostname.

  This condition occurs because the ping application does not support VRF Domain Name System (DNS) resolution. The ping application need to be extended to support VRF-aware DNS resolution.

  There are no known workarounds.

- CSCsq25196

  Border Gateway Protocol (BGP) Non-Stop Forwarding Graceful Restart (NSF-GR) does not work in a scaled setup on a Cisco ASR 1000 Router Series if the convergence time is more than 10 minutes.

  There are no known workarounds.

- CSCsq35705

  The cbQosPoliceCfgTable is failing for some configurations on a Cisco ASR 1000 Series Router. When **confirm burst** and **exceed burst** are not configured explicitly, the cbQosPoliceCfgTable is not getting populated.

  Workaround: Configure **confirm burst** and **exceed burst** explicitly, and the cbQosPoliceCfgTable will get populated as expected.

- 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 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 (first interface that is used in spd_if_bind_a() after a reload).

- 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.

- CSCsq75133

  When Bidirectional Forwarding Detection (BFD) echo mode (the default mode) and Unicast Reverse Path Forwarding (uRPF) are both enabled on an interface on a Cisco ASR 1000 Series Router, traceback of bfd_get_bfd_idb is seen on the standby RP.

  Workaround: Disable echo mode on the interface using the **no bfd echo** command. For example:

  ```
  Router(config-if)# no bfd echo
  ```

- 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.

- CSCsq90358

  On a Cisco ASR 1000 Series Router, the ESP may reload when 4K IPSec tunnels are configured with Internet Key Exchange (IKE) and IPSec lifetimes that are shorter than the default lifetimes. (The default IKE lifetime is 24 hours, and the default IPSec lifetime is 60 minutes.)

  Workaround: Either configure the IKE lifetime to be the default value (24 hours) or longer, and configure the IPSec lifetime to be the default value (60 minutes) or longer, or reduce the total number of tunnels to 2K. Future software upgrades may reduce this limitation.

- 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 and H.323 protocol calls can not be made after a prolonged run of traffic with these protocols on a Cisco ASR 1000 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.

- CSCsr03480

  When a Cisco ASR 1006 Router with a redundant RP and a redundant ESP has a large running-config, the standby ESP can unexpectedly reload when additional configurations are added to the existing running-config. This condition has been seen with the following configuration:

  - 1K IPSec sessions (250 over POS/Frame-Relay, 750 over VLANs)
  - 1 MLPPP link with QoS
  - 2 VLANs with hierarchical QoS

  - 2K SIP/Skinny sessions
  - 250 GRE tunnels with NAT, NetFlow, OSPF, and RIP

  The reload occurred when 250 Gigabit Ethernet VLANs were added to the original configuration. It is possible that this condition may occur under other scenarios.

  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.

- 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.

- CSCsr51882

  The 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.

- CSCsr53669

  The forward packet counter displayed by the **show ipv6 traffic** command on a Cisco ASR 1000 Series Router is incremented when an IPv6 ICMP packet is generated by the RP. This forward counter should only be incremented when a packet is forwarded by the router.

  There are no known workarounds.

- CSCsr56775

  On a Cisco ASR 1000 Series Router with Hierarchical QoS applied, if a policer is configured on the parent and child policies, no **shape** or **bandwidth** commands are configured, and then the child policy is removed, the parent policy will not be applied.

  There are no known workarounds.

- 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 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.

- 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.

- CSCsr93102

  A Copper GE interface on a Cisco ASR 1000 Series Router goes down after a router reload.

  This condition occurs when the interface speed is configured as 100Mbps and auto-negotiation is disabled. After the reload, the interface configuration is not getting re-applied. As a result, the link-protocol goes down.

  Workaround: Perform a **shut/no shut** of the interface to bring back the link.

- CSCsr94078

  The presence of Border Gateway Protocol (BGP) routes on a Cisco ASR 1000 Series Router may increase the time for the Interior Gateway Protocol (IGP) (ISIS or OSPF) to converge and update the forwarding table following a network failure.

  This condition occurs if the outgoing interface to the nexthop of the BGP prefixes is changed due to the convergence.

  There are no known workarounds.

  Further Problem Description: The magnitude of the convergence time increase is probably dependant on the number of BGP routes.

- 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.

- CSCsr99022

  When a virtual-template interface is removed and then re-configured on a Cisco ASR 1000 Series Router, the system fails to create the virtual-template interface.

  Workaround: Do not remove the virtual-template interface.

- CSCsu01606

  A Border Gateway Protocol (BGP) PE-PE session on a Cisco ASR 1000 Series Router gets stuck in the closing state for 5-10 minutes after the core link is shut.

  This condition was observed on a l3 VPN setup with BGP multipath configured that included 2 Interior Gateway Protocol (IGP) equal cost paths in the core.

  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.

- 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.

- 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.

- 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.

- CSCsu68057

  On a Cisco ASR 1000 Series Router, an IOSd reset occurs while running an automated script that executes the **no cns config initial** command when the primary interface out of the device is shutdown. When the **no cns config initial** command is executed manually, no reset is observed.

  Workaround: Instead of using the **no cns config partial** command in the script, use the following complete command:

  no cns config initial {*ip-address* | *host-name*} [**encrypt**] [*port-number*] [**page** *page*] [**syntax-check**] [**no-persist**] [**source** *ip-address*] [**status** *url*] [**event**] [**inventory**]

- CSCsu75596

  The ESP on a Cisco ASR 1000 Series Router may reload if a neighboring interface configured 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 the OSPF configuration and stop traffic while performing this action.

- 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 2.1.2

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.1.2.

- CSCsl49274

  A Cisco ASR 1000 Series Router may reset when the **show interface random-detect** command is executed.

  This condition occurs only when a policy map is configured with Weighted Random Early Detection (WRED) in the class-default class, and the policy map is applied to an interface.

  Workaround: Use the **show policy-map interface** command instead of the **show interface random-detect** command.

  Further Problem Description: The **show interface random-detect** command is a legacy QoS command and is not supported on the Cisco ASR 1000 Series Router.

- CSCsm49243

  On a Cisco ASR 1000 Series Router, **ip dhcp relay** commands (**ip dhcp relay information option server-id-override** and **ip dhcp relay source-interface Loopback0**) configured under interface range may not synchronize over to the newly active Route Processor (RP) after switchover.

  Workaround: Instead of using range commands, configure the interfaces individually.

- CSCso38119

  On a Cisco ASR 1000 Series Router, when control plane changes are made to Quality of Service (QoS), or subinterfaces are added that have a service policy applied when the physical interface associated with the control plane changes is over-subscribed, the following error message is reported on the console:

  ```
  CPPBQS-3-QMOVEFAIL: F0: cpp_cp: CPP 0 schedule InterfaceSchedule queue move failed
  (0xa6090402) - SEID=0x141 SID=0X280C1
  ```

  This severe condition will prohibit further configuration changes and cause inconsistencies between the control plane and data plane.

  Workaround: Avoid making control plane changes involving QoS when the physical interface associated with the changes is over-subscribed.

- CSCso71857

  A Packet-over-SONET (POS) SPA on the Cisco ASR 1000 Series Router incorrectly reports a line alarm indication signal (LAIS) alarm as a Section Bit Interleaved Parity alarm and issues the following error message:

  ```
  *Apr 9 11:09:47: %ASR1000_RP_SONET_ALARM-6-POS: ASSERT CRITICAL POS0/2/1 Section Bit
  Interleaved Parity
  ```

  There are no known workarounds.

- CSCso73923

  On a Cisco ASR 1000 Series Router, an unexpected reload of the Embedded Services Processor (ESP) may be seen if fair-queue is added to or deleted from an existing policy-map.

  This reload has been observed when a hierarchical Quality of Service (QoS) policy was modified to apply the **fair-queue** command as part of the existing child policy.

  Workaround: Detach the service-policy prior to modification, then re-attach the service-policy back to the interface.

- CSCsq08697

  The following error messages are seen on the RP console of a Cisco ASR 1000 Series Router during router boot up after upgrading from Cisco IOS XE Release 2.0 to Cisco IOS XE Release 2.1:

```
plim qos input map ip dscp  32  queue low-latency
% Invalid input detected at '^' marker
plim qos input map ipv6 tc  32  queue low-latency
% Invalid input detected at '^' marker
```

  This condition occurs because in the Cisco IOS XE Release 2.0 release of Cisco ASR 1000 software, the high priority queue for the physical layer interface module (PLIM) QoS at the input of an interface is configured using the using the **low-latency** keyword as shown below:

```
Router(config-if)# plim qos input queue ?
0            Low priority queue
low-latency  High priority queue
Router(config-if)#
Router(config-if)# plim qos input map ip dscp ef queue ?
0            Low priority queue
low-latency  High priority queue
Router(config-if)#
Router(config-if)# plim qos input map ipv6 tc ef queue ?
0            Low priority queue
low-latency  High priority queue
Router(config-if)#
```

  In contrast, beginning with Cisco IOS XE Release 2.1, the high priority queue for PLIM QoS at the input of an interface is configured using **strict-priority** keyword as shown below:

```
Router(config-if)# plim qos input queue ?
0                Low priority queue
strict-priority  High priority queue
Router(config-if)#
Router(config-if)# plim qos input map ip dscp ef queue ?
0                Low priority queue
strict-priority  High priority queue
Router(config-if)#
Router(config-if)# plim qos input map ipv6 tc ef queue ?
0                Low priority queue
strict-priority  High priority queue
Router(config-if)#
```

  Workaround: Reconfigure the PLIM QoS input map for an interface after the software upgrade using the **strict-priority** keyword instead of the **low-latency** keyword, and save the new configuration.

- CSCsq11427

  If Point-to-Point Protocol (PPP) authorization is in use on a Cisco ASR 1000 Series Router, a small amount of memory leaks for each PPP connection processed by the router.

  There are no known workarounds.

- CSCsq72274

  On a Cisco ASR 1000 Router, the audio port information (in the SDP) may not be translated correctly for an inside-to-side call with a Port Address Translation (PAT) or an interface overload Network Address Translation (NAT) configuration.

  There are no known workarounds.

- CSCsq77500

  The MEM_MGR-3-MALLOC_NO_MEM message appears on the console of a Cisco ASR 1000 Series Router.

  This condition occurs because the IP packet passing through the generic routing encapsulation (GRE) tunnel is bigger in size than the IP Maximum Transmission Unit (MTU) defined for that tunnel interface. If IP fragmentation continues for the GRE tunnel, eventually ESP memory will be used up.

  There are no known workarounds.

- CSCsq79348

  When a Cisco ASR 1000 Series Router is running IPSec with Network Address Translation (NAT), the following message may appear on the standby ESP when the IPSec session is created:

  ```
  CPP-NAT:NAT-3-HA_COULD_NOT_FIND_SESS
  ```

  This message indicates that not all the IPSec data was transferred properly to the standby ESP. As a result, if a switchover occurs, the corresponding IPSec sessions will have to be reestablished.

  There are no known workarounds.

- CSCsq87265

  A Cisco ASR 1000 Series Router may experience an unexpected system reload during L2TP Network Server (LNS) session establishment.

  This condition can occur on a router that is configured as an L2TP Network Server (LNS) when the subscriber IP address overlaps with a tunnel peer IP address as in the following example:

  ```
  Router(config)# interface TenGigabitEthernet0/2/0
  Router(config-if)# ip address 10.20.20.1 255.255.0.0
  Router(config-if)# exit
  Router(config)# interface Virtual-Template 1
  Router(config-if)# peer default ip address pool default
  Router(config-if) #exit
  Router(config)# ip local pool default 10.20.20.2 10.20.20.254
  ```

  Workaround: Configure the subscriber address pool so that it does not overlap with the tunnel peer IP address.

- CSCsq96258

  The Embedded Services Processor (ESP) software on a Cisco ASR 1000 Series Router may reload with a series of memory messages after a route processor (RP) switchover event.

  This condition can occur occasionally when the system is configured with a total of 500K prefixes, 1K VRFs, and 1K eBGP sessions during an RP switchover.

  Workaround: Reduce the number of prefixes (or routes) to below 500K.

Open Caveats—Cisco IOS XE Release 2.1.1

This section documents possible unexpected behavior by Cisco IOS XE Release 2.1.1

- CSCsl49274

  A Cisco ASR 1000 Series Router may reset when the **show interface random-detect** command is executed.

  This condition occurs only when a policy map is configured with Weighted Random Early Detection (WRED) in the class-default class, and the policy map is applied to an interface.

  Workaround: Use the **show policy-map interface** command instead of the **show interface random-detect** command.

  Further Problem Description: The **show interface random-detect** command is a legacy QoS command and is not supported on the Cisco ASR 1000 Series Router.

- CSCsm49243

  On a Cisco ASR 1000 Series Router, **ip dhcp relay** commands (**ip dhcp relay information option server-id-override** and **ip dhcp relay source-interface Loopback0**) configured under interface range may not synchronize over to the newly active route processor (RP) after switchover.

  Workaround: Instead of using range commands, configure the interfaces individually.

- CSCsm55507

  On a Cisco ASR 1000 Series Router, when the IP MTU on a Generic Routing Encapsulation (GRE) tunnel interface exceeds that on the physical interface carrying tunnel traffic, the traffic requiring fragmentation may be dropped over time.

  Workaround: Configure an IP MTU on the tunnel interface no greater than that on the physical interface carrying tunnel traffic.

- 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, and various control plane functions such as Session Border Controller (SBC) call setup may not function as expected.

  Workaround: Reduce the **show run** command output to a file for post-processing.

- CSCso38119

  On a Cisco ASR 1000 Series Router, when control plane changes are made to Quality of Service (QoS), or subinterfaces are added that have a service policy applied when the physical interface associated with the control plane changes is over-subscribed, the following error message is reported on the console:

  ```
  CPPBQS-3-QMOVEFAIL: F0: cpp_cp: CPP 0 schedule InterfaceSchedule queue move failed
  (0xa6090402) - SEID=0x141 SID=0X280C1
  ```

  This severe condition will prohibit further configuration changes and cause inconsistencies between the control plane and data plane.

  Workaround: Avoid making control plane changes involving QoS when the physical interface associated with the changes is over-subscribed.

- CSCso61824

  Under rare conditions, a SPA fails to come online when the Cisco ASR 1000 Series Router is reloaded when the Route Processor (RP) is busy processing a large configuration. The SPA process experiences multiple resets.

  Workaround: To recover from the SPA failure condition, reload the SIP.

- CSCso71857

  A Packet-over-SONET (POS) SPA on the Cisco ASR 1000 Series Router incorrectly reports a line alarm indication signal (LAIS) alarm as a Section Bit Interleaved Parity alarm and issues the following error message:

  ```
  *Apr 9 11:09:47: %ASR1000_RP_SONET_ALARM-6-POS: ASSERT CRITICAL POS0/2/1 Section Bit
  Interleaved Parity
  ```

  There are no known workarounds.

- CSCso73923

  On a Cisco ASR 1000 Series Router, an unexpected reload of the Embedded Services Processor (ESP) may be seen if fair-queue is added to or deleted from an existing policy-map.

  This reload has been observed when a hierarchical Quality of Service (QoS) policy was modified to apply the **fair-queue** command as part of the existing child policy.

  Workaround: Detach the service-policy prior to modification, then re-attach the service-policy back to the interface.

- CSCsq08067

  On a Cisco ASR 1000 Series Router, if the **nbar protocol-discovery** command is configured on multiple interfaces (for example, 200) using the **interface range** command, then the **nbar protocol-discovery** configuration is removed from all VLANs except the first VLAN after an RP switchover.

  This condition occurs after an RP switchover on the Cisco ASR 1006 Router, or an IOSd switchover on the Cisco ASR 1004 Router.

  Workaround: Instead of using the **interface range** command, configure the **nbar protocol-discovery** command for each interface individually.

- CSCsq08697

  The following error messages are seen on the RP console of a Cisco ASR 1000 Series Router during router boot up after upgrading from Cisco IOS XE Release 2.0 to Cisco IOS XE Release 2.1:

  ```
  plim qos input map ip dscp  32  queue low-latency
  % Invalid input detected at '^' marker
  plim qos input map ipv6 tc  32  queue low-latency
  % Invalid input detected at '^' marker
  ```

  This condition occurs because in the Cisco IOS XE Release 2.0 release of Cisco ASR 1000 software, the high priority queue for the physical layer interface module (PLIM) QoS at the input of an interface is configured using the using the **low-latency** keyword as shown below:

  ```
  Router(config-if)# plim qos input queue ?
  0            Low priority queue
  low-latency  High priority queue
  Router(config-if)#
  Router(config-if)# plim qos input map ip dscp ef queue ?
  0            Low priority queue
  low-latency  High priority queue
  Router(config-if)#
  Router(config-if)# plim qos input map ipv6 tc ef queue ?
  ```

```
0            Low priority queue
low-latency  High priority queue
Router(config-if)#
```

In contrast, beginning with Cisco IOS XE Release 2.1, the high priority queue for PLIM QoS at the input of an interface is configured using **strict-priority** keyword as shown below:

```
Router(config-if)# plim qos input queue ?
0               Low priority queue
strict-priority  High priority queue
Router(config-if)#
Router(config-if)# plim qos input map ip dscp ef queue ?
0               Low priority queue
strict-priority  High priority queue
Router(config-if)#
Router(config-if)# plim qos input map ipv6 tc ef queue ?
0               Low priority queue
strict-priority  High priority queue
Router(config-if)#
```

Workaround: Reconfigure the PLIM QoS input map for an interface after the software upgrade using the **strict-priority** keyword instead of the **low-latency** keyword, and save the new configuration.

- CSCsq11013

  The **show ip route vrf** command shows active VPN routes for Border Gateway Protocol (BGP) sessions that are in the “Idle” state.

  There are no known workarounds.

- CSCsq11427

  If Point-to-Point Protocol (PPP) authorization is in use on a Cisco ASR 1000 Series Router, a small amount of memory leaks for each PPP connection processed by the router.

  There are no known workarounds.

- CSCsq22332

  After provisioning different name servers in the global IP view and within a virtual routing and forwarding (VRF) instance on a Cisco ASR 1000 Series Router, a ping to a host within the VRF uses the name server in the global space to attempt to resolve the hostname.

  This condition occurs because the ping application does not support VRF Domain Name System (DNS) resolution. The ping application need to be extended to support VRF-aware DNS resolution.

  There are no known workarounds.

- CSCsq25196

  Border Gateway Protocol (BGP) Non-Stop Forwarding Graceful Restart (NSF-GR) does not work in a scaled setup on a Cisco ASR 1000 Router Series if the convergence time is more than 10 minutes.

  There are no known workarounds.

- CSCsq35705

  The cbQosPoliceCfgTable is failing for some configurations on a Cisco ASR 1000 Series Router. When **confirm burst** and **exceed burst** are not configured explicitly, the cbQosPoliceCfgTable is not getting populated.

  Workaround: Configure **confirm burst** and **exceed burst** explicitly, and the cbQosPoliceCfgTable will get populated as expected.

- 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 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 (first interface that is used in spd_if_bind_a() after a reload).

- CSCsq41016

  When an ESP switchover occurs during the time in which an IPSec Dynamic Virtual Tunnel Interface (DVTI) tunnel is being built on a Cisco ASR 1006 Router, many existing tunnels and all new tunnels will stop forwarding traffic.

  Workaround: Use a dynamic crypto map instead of DVTI.

- 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.

- CSCsq72274

  On a Cisco ASR 1000 Router, the audio port information (in the SDP) may not be translated correctly for an inside-to-side call with a Port Address Translation (PAT) or an interface overload Network Address Translation (NAT) configuration.

  There are no known workarounds.

- CSCsq75133

  When Bidirectional Forwarding Detection (BFD) echo mode (the default mode) and Unicast Reverse Path Forwarding (uRPF) are both enabled on an interface on a Cisco ASR 1000 Series Router, traceback of bfd_get_bfd_idb is seen on the standby RP.

  Workaround: Disable echo mode on the interface using the **no bfd echo** command. For example:

  ```
  Router(config-if)# no bfd echo
  ```

- CSCsq77500

  The MEM_MGR-3-MALLOC_NO_MEM message appears on the console of a Cisco ASR 1000 Series Router.

  This condition occurs because the IP packet passing through the generic routing encapsulation (GRE) tunnel is bigger in size than the IP Maximum Transmission Unit (MTU) defined for that tunnel interface. If IP fragmentation continues for the GRE tunnel, eventually ESP memory will be used up.

  There are no known workarounds.

- CSCsq77838

  A memory leak can occur in the Cisco 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 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.

- CSCsq79348

  When a Cisco ASR 1000 Series Router is running IPSec with Network Address Translation (NAT), the following message may appear on the standby ESP when the IPSec session is created:

  ```
  CPP-NAT:NAT-3-HA_COULD_NOT_FIND_SESS
  ```

  This message indicates that not all the IPSec data was transferred properly to the standby ESP. As a result, if a switchover occurs, the corresponding IPSec sessions will have to be reestablished.

  There are no known workarounds.

- CSCsq81270

  Open Shortest Path First (OSPF) adjacency is not established on a Cisco ASR 1000 Series Router with a point-to-multipoint broadcast network.

  There are no known workarounds.

- CSCsq87265

  A Cisco ASR 1000 Series Router may experience an unexpected system reload during L2TP Network Server (LNS) session establishment.

  This condition can occur on a router that is configured as an L2TP Network Server (LNS) when the subscriber IP address overlaps with a tunnel peer IP address as in the following example:

  ```
  Router(config)# interface TenGigabitEthernet0/2/0
  Router(config-if)# ip address 10.20.20.1 255.255.0.0
  Router(config-if)# exit
  Router(config)# interface Virtual-Template 1
  Router(config-if)# peer default ip address pool default
  Router(config-if) #exit
  Router(config)# ip local pool default 10.20.20.2 10.20.20.254
  ```

  Workaround: Configure the subscriber address pool so that it does not overlap with the tunnel peer IP address.

- CSCsq90358

  On a Cisco ASR 1000 Series Router, the ESP may reload when 4K IPSec tunnels are configured with Internet Key Exchange (IKE) and IPSec lifetimes that are shorter than the default lifetimes. (The default IKE lifetime is 24 hours, and the default IPSec lifetime is 60 minutes.)

  Workaround: Either configure the IKE lifetime to be the default value (24 hours) or longer, and configure the IPSec lifetime to be the default value (60 minutes) or longer, or reduce the total number of tunnels to 2K. Future software upgrades may reduce this limitation.

- CSCsq96258

  The ESP software on a Cisco ASR 1000 Series Router may reload with a series of memory messages after an RP switchover event.

  This condition can occur occasionally when the system is configured with a total of 500K prefixes, 1K VRFs, and 1K eBGP sessions during an RP switchover.

  Workaround: Reduce the number of prefixes (or routes) to below 500K.

- 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 and H.323 protocol calls can not be made after a prolonged run of traffic with these protocols on a Cisco ASR 1000 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.

- CSCsr03480

  When a Cisco ASR 1006 Router with a redundant RP and a redundant ESP has a large running-config, the standby ESP can unexpectedly reload when additional configurations are added to the existing running-config. This condition has been seen with the following configuration:

  - 1K IPSec sessions (250 over POS/Frame-Relay, 750 over VLANs)
  - 1 Multilink PPP(MLPPP) link with QoS
  - 2 VLANs with hierarchical QoS
  - 2K SIP/Skinny sessions
  - 250 GRE tunnels with NAT, NetFlow, OSPF, and RIP

  The reload occurred when 250 Gigabit Ethernet VLANs were added to the original configuration. It is possible that this condition may occur under other scenarios.

  There are no known workarounds.

  Further Problem Description: This problem occurs because after an RP failover, the AOM object under fman-fp, takes up more memory than it had previously. There is no leak, and the memory will not increase on subsequent failovers. The increase only occurs during the first failover. If your configuration is already approaching the maximum memory available on the ESP, you might run into this issue on RP failover.

- CSCsu05743

  When performing an In Service Software Upgrade (ISSU) between any two versions of Cisco IOS XE Release 2.1.0 and 2.1.1 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.

Resolved Caveats—Cisco IOS XE Release 2.1.1

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.1.1.

- CSCsm05024

  After running traffic for an extended period of time on a Cisco ASR 1000 Series Router, a Route Processor (RP) switchover may result in a reload of the new standby RP when the RP attempts to synchronize the configuration.

  After an auto-reload, the standby RP again functions as expected.

  There are no known workarounds.

- CSCsm74141

  On a Cisco ASR 1000 Series Router, successive copying of qos configuration including issuing the **match access-group** command to the running configuration leads to duplicate entries for the match access-group clause.

  Workaround: This issue is strictly a **show configuration** issue and has no functional impact.

- CSCso16581

  The TIE on line interfaces that use network clocking, such as OC3 and OC12, can oscillate and fail to meet the 100 second settling time requirement.

  This condition can occur when the network clock input (the source of timing distribution for the box) undergoes rapid changes in frequency offset. Note that this is a rare and unusual condition but still permissible. A 10 PPM delta (+5 to -5 PPM) across 10 seconds can result in a failure to meet the TIE in this case.

  Workaround: The problem can be mitigated by ensuring that there is no rapid frequency offset change on the reference clock. There is no full workaround.

- CSCso77028

  On Packet-over-SONET (POS) interfaces on a Cisco ASR 1000 Series Router with Network Based Application Recognition (NBAR) configured (Protocol discovery and/or service policies), changing the NBAR configuration, then repetitively adding and/or removing NetFlow may cause the Embedded Services Processor (ESP) to reload. The reload may occur during or after the point at which NetFlow is enabled or disabled.

  Workaround: When NBAR and NetFlow are configured on a POS interface, allow a delay of 30 seconds or more between removing the NBAR configuration and the configuration/de-configuration of NetFlow.

- CSCso81177

  On a Cisco ASR 1000 Series Router, if Network Address Translation (NAT) is configured immediately after Network Based Application Recognition (NBAR) is de-configured, an unpredictable internal state can result.

  Workaround: Configure NAT before de-configuring NBAR, or wait until all NBAR links are removed or expired.

- CSCso83252

  Connecting multiple IPSec tunnels at the same time or in quick succession using a Dynamic Virtual Tunnel Interface (DVTI) configuration on a Cisco ASR 1000 Series Router may result in some tunnels not coming up.

  Workaround: Manually remove the failed tunnels, and reconnect each tunnel one at a time.

- CSCso86721

  On a Cisco ASR 1000 Series Router if a hierarchical policy-map is configured on a parent shaper, and a priority class with percent police is configured on a child policy that is attached to a subinterface, changing the parent shape rate while the policy is attached to the interface does not translate to a change in the police cir on the child.

  Workaround: Remove the policy from the interface and reattach it.

- CSCso92930

  With Authentication, Authorization, and Accounting (AAA) accounting enabled on a Cisco ASR 1000 Series Router, the available memory Route Processor (RP) decreases over time as subscribers connect and disconnect.

  This condition is observed when the Cisco ASR 1000 Series Router is functioning as an L2TP Access Concentrator (LAC) or L2TP Network Server (LNS), and AAA accounting is enabled for tunnel, session, and Point-to-Point Protocol (PPP).

  Workaround: If the available memory decrease impacts system functions, you may disable AAA accounting.

- CSCso97208

  On a Cisco ASR 1000 Series Router, repeatedly issuing **shut** and **no shut** commands on multilink bundles with multiple member links and a Quality of Service (QoS) service policy attached may trigger an unexpected reload of the Embedded Services Processor (ESP).

  Workaround: To avoid this condition, pause 5 seconds or more between the **shut** and **no shut** operations for individual multilink bundles with a QoS service-policy attached.

- CSCso97651

  On a Cisco ASR 1000 Series Router, running stateful traffic over dynamic IPSec tunnels for an extended period may lead to an unexpected reload of the Embedded Services Processor (ESP).

  Workaround: Use static IPSec tunnels instead of dynamic tunnels, if applicable.

- CSCso98733

  On a Cisco ASR 1000 Series Router, removing a Gateway Load Balancing Protocol (GLBP) configuration may cause a failure upon the Route Processor (RP) switchover, causing an outage of the router and a subsequent reload of both RPs.

  Workaround: Avoid removing a GLBP configuration after it is configured.

- CSCso98929

  Error trace messages are generated when Network Based Application Recognition (NBAR) traffic is run during a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

  Further Problem Description: The error trace is informational only and has no functional impact.

- CSCso99244

  On a Cisco ASR 1000 Series Router, an IOSd reset occurs when an attempt is made to attach an already configured Quality of Service (QoS) service policy to a zone-pair.

  Workaround: Ensure that any service policies that are to be attached to a zone-pair are all created as inspect service policies using the **policy-map type inspect** command.

- CSCso99480

  On a Cisco ASR 1000 Series Router with Route Processor (RP)/Embedded Services Processor (ESP) redundancy, the standby ESP may reload while building 2K Dynamic Virtual Tunnel Interface (DVTI) IPSec tunnels.

  Workaround: Use a dynamic crypto map instead of DVTI.

- CSCsq01759

  When an IPSec tunnel is configured between a Cisco ASR 1000 Series Router and a remote peer using tunnel interfaces through a network address translation (NAT) device, the router drops User Datagram Protocol (UDP) encapsulated encrypted packets

  This condition affects the following features:

  - IPSec/GRE with NAT
  - DMVP with NAT
  - VTI with NAT

  Workaround: Do not configure IPSec on tunnel interfaces.

- CSCsq03423

  On a Cisco ASR 1006 Router with two Cisco ASR1000-ESP10 boards, if the **clear ip tcp header-compression** or **clear ip rtp header-compression** command is executed after a Cisco ASR1000-ESP10 switchover, the new standby Cisco ASR1000-ESP10 may reset. The newly active Cisco ASR1000-ESP10 functions correctly after the switchover.

  There are no known workarounds.

- CSCsq03572

  On a Cisco ASR 1000 Series Router, an attempt to copy a Quality of Service (QoS) policy configuration to the running configuration using the Trivial File Transfer Protocol (TFTP) does not download the policy properly when traffic to the serial interfaces is enabled for FRF12.

  Workaround: Apply the QoS policy configuration without traffic over the interfaces.

Open Caveats—Cisco IOS XE Release 2.1.0

This section documents possible unexpected behavior by Cisco IOS XE Release 2.1.0.

- CSCsl49274

  A Cisco ASR 1000 Series Router may reset when the **show interface random-detect** command is executed.

  This condition occurs only when a policy map is configured with Weighted Random Early Detection (WRED) in the class-default class, and the policy map is applied to an interface.

  Workaround: Use the **show policy-map interface** command instead of the **show interface random-detect** command.

  Further Problem Description: The **show interface random-detect** command is a legacy QoS command and is not supported on the Cisco ASR 1000 Series Router.

- CSCsm05024

  After running traffic for an extended period of time on a Cisco ASR 1000 Series Router, a Route Processor (RP) switchover may result in a reload of the new standby RP when the RP attempts to synchronize the configuration.

  After an auto-reload, the standby RP again functions as expected.

  There are no known workarounds.

- CSCsm05560

  Default wred thresholds are calculated when wred instance is created. Once wred instance is configured with default thresholds, change in class bandwidth/queue-limit does not re-calculate default threshold values unless wred instance is removed and re-installed

  Workaround: Is to remove and re-install WRED feature.

- CSCsm49243

  On a Cisco ASR 1000 Series Router, **ip dhcp relay** commands (**ip dhcp relay information option server-id-override** and **ip dhcp relay source-interface Loopback0**) configured under interface range may not synchronize over to the newly active Route Processor (RP) after switchover.

  Workaround: Instead of using range commands, configure the interfaces individually.

- CSCsm55507

  On a Cisco ASR 1000 Series Router, when the IP MTU on a Generic Routing Encapsulation (GRE) tunnel interface exceeds that on the physical interface carrying tunnel traffic, the traffic requiring fragmentation may be dropped over time.

  Workaround: Configure an IP MTU on the tunnel interface no greater than that on the physical interface carrying tunnel traffic.

- CSCsm74141

  On a Cisco ASR 1000 Series Router, successive copying of qos configuration including issuing the **match access-group** command to the running configuration leads to duplicate entries for the match access-group clause.

  Workaround: This issue is strictly a **show configuration** issue and has no functional impact.

- 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, and various control plane functions such as Session Border Controller (SBC) call setup may not function as expected.

  Workaround: Reduce the **show run** command output to a file for post-processing.

- CSCso16581

  The TIE on line interfaces that use network clocking, such as OC3 and OC12, can oscillate and fail to meet the 100 second settling time requirement.

  This condition can occur when the network clock input (the source of timing distribution for the box) undergoes rapid changes in frequency offset. Note that this is a rare and unusual condition but still permissible. A 10 PPM delta (+5 to -5 PPM) across 10 seconds can result in a failure to meet the TIE in this case.

  Workaround: The problem can be mitigated by ensuring that there is no rapid frequency offset change on the reference clock. There is no full workaround.

- CSCso38119

  On a Cisco ASR 1000 Series Router, when control plane changes are made to Quality of Service (QoS), or subinterfaces are added that have a service policy applied when the physical interface associated with the control plane changes is over-subscribed, the following error message is reported on the console:

  ```
  CPPBQS-3-QMOVEFAIL: F0: cpp_cp: CPP 0 schedule InterfaceSchedule queue move failed
  (0xa6090402) - SEID=0x141 SID=0X280C1
  ```

  This severe condition will prohibit further configuration changes and cause inconsistencies between the control plane and data plane.

  Workaround: Avoid making control plane changes involving QoS when the physical interface associated with the changes is over-subscribed.

- CSCso61824

  Under rare conditions, a SPA fails to come online when the Cisco ASR 1000 Series Router is reloaded when the Route Processor (RP) is busy processing a large configuration. The SPA process experiences multiple resets.

  Workaround: To recover from the SPA failure condition, reload the SIP.

- CSCso71857

  A Packet-over-SONET (POS) SPA on the Cisco ASR 1000 Series Router incorrectly reports a line alarm indication signal (LAIS) alarm as a Section Bit Interleaved Parity alarm and issues the following error message:

  ```
  *Apr 9 11:09:47: %ASR1000_RP_SONET_ALARM-6-POS: ASSERT CRITICAL POS0/2/1 Section Bit
  Interleaved Parity
  ```

  There are no known workarounds.

- CSCso73923

  On a Cisco ASR 1000 Series Router, an unexpected reload of the Embedded Services Processor (ESP) may be seen if fair-queue is added to or deleted from an existing policy-map.

  This reload has been observed when a hierarchical Quality of Service (QoS) policy was modified to apply the **fair-queue** command as part of the existing child policy.

  Workaround: Detach the service-policy prior to modification, then re-attach the service-policy back to the interface.

- CSCso77028

  On Packet-over-SONET (POS) interfaces on a Cisco ASR 1000 Series Router with Network Based Application Recognition (NBAR) configured (Protocol discovery and/or service policies), changing the NBAR configuration, then repetitively adding and/or removing NetFlow may cause the Embedded Services Processor (ESP) to reload. The reload may occur during or after the point at which NetFlow is enabled or disabled.

  Workaround: When NBAR and NetFlow are configured on a POS interface, allow a delay of 30 seconds or more between removing the NBAR configuration and the configuration/de-configuration of NetFlow.

- CSCso81177

  On a Cisco ASR 1000 Series Router, if Network Address Translation (NAT) is configured immediately after Network Based Application Recognition (NBAR) is de-configured, an unpredictable internal state can result.

  Workaround: Configure NAT before de-configuring NBAR, or wait until all NBAR links are removed or expired.

- CSCso83252

  Connecting multiple IPSec tunnels at the same time or in quick succession using a Dynamic Virtual Tunnel Interface (DVTI) configuration on a Cisco ASR 1000 Series Router may result in some tunnels not coming up.

  Workaround: Manually remove the failed tunnels, and reconnect each tunnel one at a time.

- CSCso86721

  On a Cisco ASR 1000 Series Router if a hierarchical policy-map is configured on a parent shaper, and a priority class with percent police is configured on a child policy that is attached to a subinterface, changing the parent shape rate while the policy is attached to the interface does not translate to a change in the police cir on the child.

  Workaround: Remove the policy from the interface and reattach it.

- CSCso92930

  With Authentication, Authorization, and Accounting (AAA) accounting enabled on a Cisco ASR 1000 Series Router, the available memory Route Processor (RP) decreases over time as subscribers connect and disconnect.

  This condition is observed when the Cisco ASR 1000 Series Router is functioning as an L2TP Access Concentrator (LAC) or L2TP Network Server (LNS), and AAA accounting is enabled for tunnel, session, and Point-to-Point Protocol (PPP).

  Workaround: If the available memory decrease impacts system functions, you may disable AAA accounting.

- CSCso97208

  On a Cisco ASR 1000 Series Router, repeatedly issuing **shut** and **no shut** commands on multilink bundles with multiple member links and a Quality of Service (QoS) service policy attached may trigger an unexpected reload of the Embedded Services Processor (ESP).

  Workaround: To avoid this condition, pause 5 seconds or more between the **shut** and **no shut** operations for individual multilink bundles with a QoS service-policy attached.

- CSCso97651

  On a Cisco ASR 1000 Series Router, running stateful traffic over dynamic IPSec tunnels for an extended period may lead to an unexpected reload of the Embedded Services Processor (ESP).

  Workaround: Use static IPSec tunnels instead of dynamic tunnels, if applicable.

- CSCso98733

  On a Cisco ASR 1000 Series Router, removing a Gateway Load Balancing Protocol (GLBP) configuration may cause a failure upon the Route Processor (RP) switchover, causing an outage of the router and a subsequent reload of both RPs.

  Workaround: Avoid removing a GLBP configuration after it is configured.

- CSCso98929

  Error trace messages are generated when Network Based Application Recognition (NBAR) traffic is run during a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

  Further Problem Description: The error trace is informational only and has no functional impact.

- CSCso99244

  On a Cisco ASR 1000 Series Router, an IOSd reset occurs when an attempt is made to attach an already configured Quality of Service (QoS) service policy to a zone-pair.

  Workaround: Ensure that any service policies that are to be attached to a zone-pair are all created as inspect service policies using the **policy-map type inspect** command.

- CSCso99480

  On a Cisco ASR 1000 Series Router with Route Processor (RP)/Embedded Services Processor (ESP) redundancy, the standby ESP may reload while building 2K Dynamic Virtual Tunnel Interface (DVTI) IPSec tunnels.

  Workaround: Use a dynamic crypto map instead of DVTI.

- CSCsq01759

  When an IPSec tunnel is configured between a Cisco ASR 1000 Series Router and a remote peer using tunnel interfaces through a network address translation (NAT) device, the router drops User Datagram Protocol (UDP) encapsulated encrypted packets

  This condition affects the following features:

  - IPSec/GRE with NAT
  - DMVP with NAT
  - VTI with NAT

  Workaround: Do not configure IPSec on tunnel interfaces.

- CSCsq03423

  On a Cisco ASR 1006 Router with two Cisco ASR1000-ESP10 boards, if the **clear ip tcp header-compression** or **clear ip rtp header-compression** command is executed after a Cisco ASR1000-ESP10 switchover, the new standby Cisco ASR1000-ESP10 may reset. The newly active Cisco ASR1000-ESP10 functions correctly after the switchover.

  There are no known workarounds.

- CSCsq03572

  On a Cisco ASR 1000 Series Router, an attempt to copy a Quality of Service (QoS) policy configuration to the running configuration using the Trivial File Transfer Protocol (TFTP) does not download the policy properly when traffic to the serial interfaces is enabled for FRF12.

  Workaround: Apply the QoS policy configuration without traffic over the interfaces.