The Cisco IOS XE Release 3S is supported for both the Cisco ASR 903 Series Aggregation Services Router and the Cisco ASR 1000 Series Aggregation Services Routers.

- **Cisco ASR 903 Series Aggregation Services Router**, page 1
- **Cisco ASR 1000 Series Aggregation Services Routers**, page 1

**Cisco ASR 903 Series Aggregation Services Router**

The Cisco ASR 903 Series Aggregation Services Router is a Cisco aggregation router product. This router uses an innovative and powerful forwarding technology known as the Cisco Carrier Ethernet ASIC.

The Cisco ASR 903 Series Router is a 6-Interface Module (IM), 3-RU, hardware-redundant chassis with two Route Switch Processor (RSP) slots, and six IM slots. It supports fully redundant RSPs that allow for full RSP hardware redundancy, NSF, ISSU, and future RSP service upgrades. The Cisco ASR 903 Series Router runs the Cisco IOS XE software and is supported since Cisco IOS XE Release 3.5S.

**Cisco ASR 1000 Series Aggregation Services Routers**

The Cisco ASR 1000 Series Aggregation Services Routers are Cisco midrange router products. These routers use an innovative and powerful hardware processor technology known as the Cisco QuantumFlow Processor.

In July 2010, the Cisco IOS XE software moved from Cisco IOS XE Release 2.6 to Cisco IOS XE Release 3.1S to introduce new hardware (ASR1000-ESP40, ASR1000-SIP40, and Cisco ASR 1013 Router) and an enhanced Cisco IOS Release 15.0(1)S software that runs on improved componentized code for Cisco IOS features.

The Cisco IOS XE release numbering scheme is modified by the addition of the suffix “S” to the release number to denote the release branch that will differentiate the different products using Cisco IOS XE release.
The underlying Cisco IOS software numbering scheme for the Cisco ASR 1000 Series Routers changes from the current numbering of 12.2(33)XNx to 15.0(1)S. This change will define simpler numbering for new feature releases (the number in parenthesis) and rebuilds. Cisco IOS Release 15S aggregates feature inheritance from the Cisco IOS Release 12.2SR. The 15.x(x)Sx releases will continue to be time-based and time-synchronized with Cisco IOS XE releases.

Table 1 lists the mappings between Cisco IOS XE 3S versions and their associated Cisco IOS versions.

<table>
<thead>
<tr>
<th>Cisco IOS XE 3S Version</th>
<th>Cisco IOS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.0S</td>
<td>15.0(1)S</td>
</tr>
<tr>
<td>3.1.1S</td>
<td>15.0(1)S1</td>
</tr>
<tr>
<td>3.1.2S</td>
<td>15.0(1)S2</td>
</tr>
<tr>
<td>3.1.3S</td>
<td>15.0(1)S3</td>
</tr>
<tr>
<td>3.1.4S</td>
<td>15.0(1)S4</td>
</tr>
<tr>
<td>3.1.4aS</td>
<td>15.0(1)S4a</td>
</tr>
<tr>
<td>3.2.0S</td>
<td>15.1(1)S</td>
</tr>
<tr>
<td>3.2.1S</td>
<td>15.1(1)S1</td>
</tr>
<tr>
<td>3.2.2S</td>
<td>15.1(1)S2</td>
</tr>
<tr>
<td>3.3.0S</td>
<td>15.1(2)S</td>
</tr>
<tr>
<td>3.3.1S</td>
<td>15.1(2)S1</td>
</tr>
<tr>
<td>3.3.2S</td>
<td>15.1(2)S2</td>
</tr>
<tr>
<td>3.4.0S</td>
<td>15.1(3)S</td>
</tr>
<tr>
<td>3.4.0aS</td>
<td>15.1(3)S0a</td>
</tr>
<tr>
<td>3.4.1S</td>
<td>15.1(3)S1</td>
</tr>
<tr>
<td>3.4.2S</td>
<td>15.1(3)S2</td>
</tr>
<tr>
<td>3.4.3S</td>
<td>15.1(3)S3</td>
</tr>
<tr>
<td>3.4.4S</td>
<td>15.1(3)S4</td>
</tr>
<tr>
<td>3.4.5S</td>
<td>15.1(3)S5</td>
</tr>
<tr>
<td>3.4.6S</td>
<td>15.1(3)S6</td>
</tr>
<tr>
<td>3.5.0S</td>
<td>15.2(1)S</td>
</tr>
<tr>
<td>3.5.1S</td>
<td>15.2(1)S1</td>
</tr>
<tr>
<td>3.5.2S</td>
<td>15.2(1)S2</td>
</tr>
</tbody>
</table>

Cisco IOS XE 3S releases inherit all Cisco IOS XE Release 2 features that were released prior to the introduction of the Cisco IOS XE Release 3.1.0S, with a few exceptions. For information about inherited features, see Release Notes for Cisco ASR 1000 Series Aggregation Services Routers for Cisco IOS XE Release 2.

The Cisco ASR 1000 Series consists of the following routers:

- The Cisco ASR 1001 Router is a small form factor router targeted for high-end branch offices needing integrated services including voice and security with high-speed connectivity (2.5 Gbps w/optimal SW license for 5 Gbps). Designed with integrated Cisco ASR1000-RP, Cisco
ASR1000-SIP, Cisco ASR1000-ESP with Nitrox running Cisco IOS XE Release 3.2S. Input/output options include Half-height SPA, 4x1GE built-in ports, factory-installed integrated daughtercard (IDC) with different options.

- The Cisco ASR 1002 Router is a 3-SPA, 2-rack-unit (RU) chassis with one Embedded Services Processor (ESP) slot that comes with the Route Processor (RP), Cisco ASR 1000 Series Shared Port Adapter Interface Processor (SIP), and four Gigabit Ethernet ports built in.
- The Cisco ASR 1002-F Router supports the same features and components as the Cisco ASR 1002 Router. In addition, the Cisco ASR 1002-F Router has an integrated 4xGE SPA interface, 2.5 GB of fixed system bandwidth, and 4 GB of DRAM.
- The Cisco ASR 1004 Router is an 8-SPA, 4-RU chassis with one ESP slot, one RP slot, and two SIP slots.
- The Cisco ASR 1006 Router is a 12-SPA, 6-RU, hardware-redundant chassis with two ESP slots, two Route Processor (RP) slots, and three SIP slots.
- The Cisco ASR 1013 Router is a 24-SPA, 3-RU, hardware-redundant chassis with two ESP slots, two RP slots, and six SIP slots that allows for full RP hardware redundancy, Nonstop Forwarding (NSF), In-Service Software Upgrade (ISSU), and future RP service upgrades.

For the single-route-processor Cisco ASR 1000 platforms, the Cisco ASR 1002 and Cisco ASR 1004, the RP has a dual Cisco IOS software option that allows these routers to use Cisco IOS software redundancy, Cisco high-availability features, NSF, and ISSUs. This option requires the Cisco ASR 1000 Series RP to have 4 GB of DRAM memory.

The Cisco ASR 1006 Router supports fully redundant RPs that allow for full RP hardware redundancy, NSF, ISSU, and future RP service upgrades.

The Cisco ASR 1013 Router extends the Cisco ASR 1000 Series Routers to a chassis that can hold six SIPs and provides superslots (more height and power) for the Cisco ASR1000-RPs (route processor) and the ASR1000-ESPs (forwarding processor).

The Cisco ASR 1000 Series Routers run the Cisco IOS XE software and introduce a distributed software architecture that moves many operating system responsibilities out of the IOS process. In this architecture, Cisco IOS, which previously was responsible for almost all of the internal software processes, now runs as one of many Cisco IOS XE processes while allowing other Cisco IOS XE processes to share responsibility for running the router.

One of the key features of the Cisco IOS XE 3.1S software is support for dual Cisco IOS software consolidated packages in a single RP for software redundancy in the 2-RU and 4-RU chassis systems. These dual Cisco IOS consolidated packages can consist of the same software consolidated packages for backup or different software consolidated packages for resilient upgrade.

**Note**

Software redundancy is not supported on the Cisco ASR 1006 Router and the Cisco ASR 1013 Router.
System Requirements for Cisco IOS XE 3S Releases

The following sections describe the system requirements for Cisco IOS XE 3S releases:

- Software Packaging on the Cisco ASR 1000 Series Routers, page 5
- Cisco IOS XE 3S Software Package Compatibility for ISSU, page 7
- Hardware Supported, page 15
- ROMmon Version Requirements, page 15
- Determining the Software Version, page 15
- Cisco IOS XE 3S to Cisco IOS Version Number Mapping, page 21
- Upgrading to a New Software Release, page 21

Software Packaging on the Cisco ASR 1000 Series Routers

The Cisco ASR 1000 Series Routers run Cisco IOS XE 3S Software and use a software packaging model consisting of:

- Consolidated packages
- Individual software subpackages within a consolidated package
- Optional software subpackages outside of consolidated packages

Each Cisco IOS XE 3S consolidated package contains a collection of individual software subpackages. Each individual software subpackage is an individual software file that controls a different element or elements of the Cisco ASR 1000 Series Router. Some individual subpackages may be installed per element (for example, per SPA).

Note

The subpackage functionality is intended for both upgrade and field support, and not all combinations of subpackages are supported.
Each individual software subpackage can be upgraded individually, or all individual software subpackages for a specific Cisco IOS XE 3S consolidated package can be upgraded as part of a complete Cisco IOS XE 3S consolidated package upgrade.

Importantly, IOS (the RPIOS individual software subpackage) is considered one of the individual software subpackages that makes up the complete Cisco IOS XE 3S consolidated package.

The following are the individual software subpackages within a consolidated package:

- **Route Processor**
  - RPBase: Provides the Route-Processor operating system.
  - RPControl: Provides the control-plane processes that interface between Cisco IOS Software and the rest of the platform.
  - RPIOS: Provides the Cisco IOS Software kernel, which is where Cisco IOS Software features are stored and run; each consolidated image variant has a different RPIOS subpackage: RPIOS-ipbase, RPIOS-ipbasek9, RPIOS-advipservices, RPIOS-advipservicesk9, RPIOS-adventservices, and RPIOS-adventservicesk9.

- **ESP**
  - ESPBase: Provides the ESP operating system and control processes, and the Cisco QuantumFlow Processor client, driver, and ucode.

- **SIP**
  - SIPBase: Provides the SIP operating system and control processes.
  - SIPSPA: Provides the SPA drivers and associated field-programmable device (FPD) image (SPA FPGA image)

A Cisco IOS XE 3S consolidated package allows users to upgrade all individual software subpackages on the router with a single Cisco IOS XE 3S image download. The Cisco IOS XE 3S consolidated packages available vary based on the Route Processor (RP1 or RP2) installed in the system and the Cisco IOS XE 3S Release.

The following are the RP1 consolidated packages:

- Cisco ASR 1000 Series RP1 IP BASE W/O CRYPTO
- Cisco ASR 1000 Series RP1 IP BASE
- Cisco ASR 1000 Series RP1 ADVANCED IP SERVICES
- Cisco ASR 1000 Series RP1 ADVANCED IP SERVICES W/O CRYPTO
- Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES
- Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES W/O CRYPTO

The following are the RP2 consolidated packages:

- Cisco ASR 1000 Series RP2 IP BASE W/O CRYPTO
- Cisco ASR 1000 Series RP2 IP BASE
- Cisco ASR 1000 Series RP2 ADVANCED IP SERVICES
The individual software subpackages within the consolidated packages cannot be downloaded from Cisco.com; only the Cisco IOS XE S consolidated packages and optional subpackages can be downloaded from Cisco.com. Users who want to run the router using individual software subpackages must first download the consolidated package from Cisco.com and extract the individual software subpackages from the consolidated package.

In addition to the individual software subpackages within a consolidated package, optional software subpackages that are not part of a consolidated package are available. Optional software subpackages are downloaded separately from Cisco.com and their installation is similar to the installation of an individual software subpackage using a provisioning file. The optional subpackage must be located in the same directory with the provisioning file and the other individual subpackage files. The optional software subpackages available vary based on the Route Processor (RP) installed in the system: RP1 or RP2:

- For the RP1, the optional software subpackage available is the Cisco ASR 1000 Series RP1 WebEx Node (asr1000rp1-sipspawmak9.version.pkg)
- For the RP2, the optional software subpackage available is the Cisco ASR 1000 Series RP2 WebEx Node (asr1000rp2-sipspawmak9.version.pkg)

**Note**

The Cisco ASR 1000 Series RP1 WebEx Node and Cisco ASR 1000 Series RP2 WebEx Node optional software subpackages are only available beginning with Cisco IOS XE Release 2.4.0 and later releases and are only supported in conjunction with a related RP-based Cisco ASR 1000 Series RPx IP BASE, Cisco ASR 1000 Series RPx ADVANCED IP SERVICES, or Cisco ASR 1000 Series RPx ADVANCED ENTERPRISE SERVICES consolidated package. These optional software subpackages are not supported with earlier Cisco IOS XE releases or with any of the non-CRYPTO consolidated packages.

**Note**

ISSU operation on the Cisco ASR 1002 and Cisco ASR 1004 systems requires the system to be operating in subpackage mode.

**Note**

USB (or any other removable media) cannot be used to boot the system into subpackage mode.

For further information about the advantages and disadvantages of running individual subpackages or a complete Cisco IOS XE 3S consolidated package, and the process of extracting the individual subpackages, see *Cisco ASR 1000 Series Aggregation Services Router Software Configuration Guide* at the following location:


---

**Cisco IOS XE 3S Software Package Compatibility for ISSU**

Cisco IOS XE Release 3.1S is an ISSU break release. In Cisco IOS XE Release 3.1S, ISSU upgrade and subpackage software upgrade from Cisco IOS XE Release 2.x to Cisco IOS XE Release 3.xS, including Release 3.1S, is not supported. The ISSU downgrade from Cisco IOS XE Release 3.xS, including Release 3.1S to 2.x, is not supported either.
ISSU upgrade and subpackage software upgrade are restarted from Cisco IOS XE Release 3.1S. Therefore, rebuilds and releases after Cisco IOS XE Release 3.1S will support ISSU and software upgrade and downgrade, based on the ISSU compatibility matrix tables. For example, ISSU upgrade and downgrade between Cisco IOS XE Release 3.1.0S (15.0(1)S) to Cisco IOS XE Release 3.xS are supported.

For information about Cisco IOS XE 3.x releases that supports ISSU and software upgrade and downgrade, based on the ISSU compatibility matrix tables in Cisco IOS XE Release 3 releases, see the “Cisco ASR 1000 Series Aggregation Services Routers Software Package Compatibility for ISSU” section in Cisco ASR 1000 Series Aggregation Services Routers Release Notes.

For information about Cisco IOS XE 2.x releases that supports ISSU and software upgrade and downgrade, based on the ISSU compatibility matrix tables in Cisco IOS XE Release 2 releases, see the "Cisco IOS XE Release Compatibility Tables" section in Release Notes for Cisco ASR 1000 Series Aggregation Services Routers for Cisco IOS XE Release 2.

---

Note

Cisco IOS XE software compatibility is between “like” images, for example, advipservicesk9 to advipservicesk9, adventerprisek9 to adventerprisek9, and so on. Cross-image-type upgrades or installations are not supported in the ISSU process. For example, you cannot upgrade ipbase to advipservicesk9 or advipservices to advipservicesk9.

---

**RP Memory Recommendations**

- Cisco ASR 903 Series Aggregation Services Router, page 8
- Cisco ASR 1000 Series Aggregation Services Routers, page 10

**Cisco ASR 903 Series Aggregation Services Router**

The Cisco IOS XE 3S images and packages available vary based on the route processor (either RSP1 or RSP1+) installed in the system:

Table 1 describes the consolidated package image, the individual software subpackage contents, and the memory recommendations.
<table>
<thead>
<tr>
<th>Platform</th>
<th>Image Name</th>
<th>Software Image</th>
<th>Individual Subpackage Contents</th>
<th>DRAM Memory</th>
</tr>
</thead>
</table>
Cisco ASR 1000 Series Aggregation Services Routers

The Cisco IOS XE 3S images and packages available vary based on the route processor (either RP1 or RP2) installed in the system:

- **Table 2** describes the RP1 consolidated package images, their individual software subpackage contents, and their memory recommendations.
- **Table 3** describes the RP1 optional subpackage images and their memory recommendations.
- **Table 4** describes the RP2 consolidated package images, their individual software subpackage contents, and their memory recommendations.
- **Table 5** describes the RP2 optional subpackage images and their memory recommendations.

Each Cisco IOS XE 3S image also contains two provisioning files: asr1000rp1-packages.image.version.conf and packages.conf. A provisioning file is used for booting only in cases where the individual modules are extracted from the Cisco IOS XE 3.1S image and then used to run the router. Either provisioning file can be used.

### Table 2  
**RP1 Memory Recommendations for the Cisco ASR 1000 Series Routers Consolidated Package Images**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Image Name</th>
<th>Software Image</th>
<th>Individual Subpackage Contents</th>
<th>DRAM Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASR 1002 Router</td>
<td>Cisco ASR 1000 Series RP1 IP BASE W/O CRYPTO</td>
<td>asr1000rp1-ipbase.version.bin</td>
<td>asr1000rp1-rpbase.version.pkg</td>
<td>4 GB (for Cisco ASR 1002 Router)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-rpcontrol.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-rpaccess.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-rpios-ipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-espbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-sipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-sipspa.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-packages-ipbase.version.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>packages.conf</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Image Name</th>
<th>Software Image</th>
<th>Individual Subpackage Contents</th>
<th>DRAM Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASR 1002 Router</td>
<td>Cisco ASR 1000 Series RP1 IP BASE</td>
<td>asr1000rp1-ipbasek9.version.bin</td>
<td>asr1000rp1-rpbase.version.pkg</td>
<td>4 GB (for Cisco ASR 1002 Router)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-rpcontrol.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-rpaccess.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-rpios-ipbasek9.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-espbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-sipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-sipspa.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-packages-ipbasek9.version.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>packages.conf</td>
<td></td>
</tr>
<tr>
<td>Platforms</td>
<td>Image Name</td>
<td>Software Image</td>
<td>Individual Subpackage Contents</td>
<td>DRAM Memory</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco ASR 1002 Router</td>
<td>Cisco ASR 1000 Series RP1 ADVANCED IP SERVICES W/O CRYPTO</td>
<td>asr1000rp1-advipservices.version.bin</td>
<td>asr1000rp1-rpbase.version.pkg</td>
<td>4 GB (for Cisco ASR 1002 Router)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-rpcontrol.version.pkg</td>
<td>2 GB–4 GB (for Cisco ASR 1004 and Cisco ASR 1006 routers)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-rpaccess.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-rpios-advipservices.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-espbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-sipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-sipspa.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-packages-advipservices.version.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>packages.conf</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 1002 Router</td>
<td>Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES W/O CRYPTO</td>
<td>asr1000rp1-adventservices.version.bin</td>
<td>asr1000rp1-rpbase.version.pkg</td>
<td>4 GB (for Cisco ASR 1002 Router)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-rpcontrol.version.pkg</td>
<td>2 GB–4 GB (for Cisco ASR 1004 and Cisco ASR 1006 routers)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-rpaccess.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-rpios-adventservices.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-espbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-sipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-sipspa.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-packages-adventservices.version.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>packages.conf</td>
<td></td>
</tr>
</tbody>
</table>
**Table 2**  
*RP1 Memory Recommendations for the Cisco ASR 1000 Series Routers Consolidated Package Images*

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Image Name</th>
<th>Software Image</th>
<th>Individual Subpackage Contents</th>
<th>DRAM Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASR 1002</td>
<td>Cisco ASR 1000 Series RP1</td>
<td>asr1000rp1-adventservicesk9.version.bin</td>
<td>asr1000rp1-rpbase.version.pkg</td>
<td>4 GB (for Cisco ASR 1002 Router)</td>
</tr>
<tr>
<td>Router</td>
<td>ADVANCED ENTERPRISE SERVICES</td>
<td></td>
<td>asr1000rp1-rpcontrol.version.pkg</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 1004</td>
<td></td>
<td></td>
<td>asr1000rp1-rpaccess.version.pkg</td>
<td>2 GB–4 GB (for Cisco ASR 1004 and Cisco ASR 1006 routers)</td>
</tr>
<tr>
<td>Router</td>
<td></td>
<td></td>
<td>asr1000rp1-rpios-adventservicesk9.version.pkg</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 1006</td>
<td></td>
<td></td>
<td>asr1000rp1-espbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td>Router</td>
<td></td>
<td></td>
<td>asr1000rp1-sipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-sipspa.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp1-packages-adventservicesk9.version.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>packages.conf</td>
<td></td>
</tr>
</tbody>
</table>

**Table 3**  
*RP1 Memory Recommendations for the Cisco ASR 1000 Series Routers Optional Subpackage Image*

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Image Name</th>
<th>Software Image</th>
<th>Flash Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASR 1002</td>
<td>Cisco ASR 1000 Series RP1 WebEx Node</td>
<td>asr1000rp1-sipspawmak9.version.XND.pkg</td>
<td>100MB</td>
</tr>
<tr>
<td>Router</td>
<td>WebEx Node</td>
<td>asr1000rp1-sipspawmak9.version.XND.pkg</td>
<td>100MB</td>
</tr>
<tr>
<td>Cisco ASR 1004</td>
<td></td>
<td>asr1000rp1-sipspawmak9.version.XND.pkg</td>
<td>100MB</td>
</tr>
<tr>
<td>Router</td>
<td></td>
<td>asr1000rp1-sipspawmak9.version.XND.pkg</td>
<td>100MB</td>
</tr>
<tr>
<td>Cisco ASR 1006</td>
<td></td>
<td>asr1000rp1-sipspawmak9.version.XND.pkg</td>
<td>100MB</td>
</tr>
<tr>
<td>Router</td>
<td></td>
<td>asr1000rp1-sipspawmak9.version.XND.pkg</td>
<td>100MB</td>
</tr>
</tbody>
</table>

1. The Cisco ASR 1000 Series RP1 WebEx Node (asr1000rp1-sipspawmak9.version.pkg) optional software subpackage is only available beginning with Cisco IOS XE Release 2.4.0 and later releases and only supported in conjunction with the Cisco ASR 1000 Series RP1 IP BASE, Cisco ASR 1000 Series RP1 ADVANCED IP SERVICES, or Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES consolidated package. This subpackage is not supported with earlier Cisco IOS XE releases or with any of the non-CRYPTO consolidated packages.

**Note**  
RP2 images are available from Cisco IOS XE Release 2.3.0.
## Table 4 RP2 Memory Recommendations for the Cisco ASR 1000 Series Routers Consolidated Package Images

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Image Name</th>
<th>Software Image</th>
<th>Individual Subpackage Contents</th>
<th>DRAM Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASR 1004</td>
<td>Cisco ASR 1000 Series RP2 IP BASE W/O CRYPTO</td>
<td>asr1000rp2-ipbase.version.bin</td>
<td>asr1000rp2-rpbase.version.pkg</td>
<td>8 GB–16 GB (for Cisco ASR 1004 and Cisco ASR 1006 and Cisco ASR 1013 routers)</td>
</tr>
<tr>
<td>Cisco ASR 1006</td>
<td></td>
<td></td>
<td>asr1000rp2-rpcontrol.version.pkg</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 1013</td>
<td></td>
<td></td>
<td>asr1000rp2-rpaccess.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-rpios-ipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-espbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-sipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-sipspa.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-packages-ipbase.version.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>packages.conf</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 1004</td>
<td>Cisco ASR 1000 Series RP2 ADVANCED IP SERVICES</td>
<td>asr1000rp2-ipbasek9.version.bin</td>
<td>asr1000rp2-rpbase.version.pkg</td>
<td>8 GB–16 GB (for Cisco ASR 1004 and Cisco ASR 1006 and Cisco ASR 1013 routers)</td>
</tr>
<tr>
<td>Cisco ASR 1006</td>
<td></td>
<td></td>
<td>asr1000rp2-rpcontrol.version.pkg</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 1013</td>
<td></td>
<td></td>
<td>asr1000rp2-rpaccess.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-rpios-ipbasek9.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-espbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-sipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-sipspa.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-packages-ipbasek9.version.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>packages.conf</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 1004</td>
<td>Cisco ASR 1000 Series RP2 ADVANCED IP SERVICES</td>
<td>asr1000rp2-advipservices.version.bin</td>
<td>asr1000rp2-rpbase.version.pkg</td>
<td>8 GB–16 GB (for Cisco ASR 1004 and Cisco ASR 1006 and Cisco ASR 1013 routers)</td>
</tr>
<tr>
<td>Cisco ASR 1006</td>
<td></td>
<td></td>
<td>asr1000rp2-rpcontrol.version.pkg</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 1013</td>
<td></td>
<td></td>
<td>asr1000rp2-rpaccess.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-rpios-advipservices.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-espbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-sipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-sipspa.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-packages-advipservices.version.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>packages.conf</td>
<td></td>
</tr>
</tbody>
</table>

---

**OL-23288-23**

**Cisco IOS XE 3S Software Package Compatibility for ISSU**
### Table 4: RP2 Memory Recommendations for the Cisco ASR 1000 Series Routers Consolidated Package Images

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Image Name</th>
<th>Software Image</th>
<th>Individual Subpackage Contents</th>
<th>DRAM Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASR 1004 Router</td>
<td>Cisco ASR 1000 Series RP2 ADVANCED IP SERVICES</td>
<td>asr1000rp2-advipservicesk9.version.bin</td>
<td>asr1000rp2-rpbase.version.pkg</td>
<td>8 GB–16 GB (for Cisco ASR 1004 Cisco ASR 1006 and Cisco ASR 1013 routers)</td>
</tr>
<tr>
<td>Cisco ASR 1006 Router</td>
<td></td>
<td></td>
<td>asr1000rp2-rpcontrol.version.pkg</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 1013 Router</td>
<td></td>
<td></td>
<td>asr1000rp2-rpaccess.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-rpios-advipservicesk9.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-espbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-sipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-sipspa.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-packages-advipservicesk9.version.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>packages.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASR 1004 Series RP2 ADVANCED ENTERPRISE SERVICES W/O CRYPTO</td>
<td>asr1000rp2-adventservices.version.bin</td>
<td>asr1000rp2-rpbase.version.pkg</td>
<td>8 GB–16 GB (for Cisco ASR 1004 Cisco ASR 1006 and Cisco ASR 1013 routers)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-rpcontrol.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-rpaccess.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-rpios-adventservices.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-espbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-sipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-sipspa.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-packages-adventservices.version.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>packages.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASR 1000 Series RP2 ADVANCED ENTERPRISE SERVICES</td>
<td>asr1000rp2-adventservicesk9.version.bin</td>
<td>asr1000rp2-rpbase.version.pkg</td>
<td>8 GB–16 GB (for Cisco ASR 1004 Cisco ASR 1006 and Cisco ASR 1013 routers)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-rpcontrol.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-rpaccess.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-rpios-adventservicesk9.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-espbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-sipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-sipspa.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr1000rp2-packages-adventservicesk9.version.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>packages.conf</td>
<td></td>
</tr>
</tbody>
</table>
Hardware Supported

Cisco IOS XE 3S releases support the following Cisco ASR 1000 Series Routers and the Cisco ASR 903 Router:

- Cisco ASR 1001 Router
- Cisco ASR 1002 Router
- Cisco ASR 1002-F Router
- Cisco ASR 1004 Router
- Cisco ASR 1006 Router
- Cisco ASR 1013 Router
- Cisco ASR 903 Router (introduced in Cisco IOS XE Release 3.5.0S)

ROMmon Version Requirements

This section describes the recommended and minimum ROMmon version requirements for Cisco IOS XE releases up to and including Cisco IOS XE Release 3.10S.

For information about recommended and minimum ROMmon version requirements see the “ROMmon Release Requirements” section in Cisco ASR 1000 Series Aggregation Services Routers Release Notes.

Determining the Software Version

This section provides information about determining the software version.

Determining the Consolidated Package Version

To determine the version of the Cisco IOS XE Software (consolidated package) running on your Cisco ASR 1000 Series Router, log in to the router and enter the show version EXEC command.
The following is sample output of the `show version` command. The actual output displayed when you run the command will vary depending on the version of the product that you are using.

```
Router# show version
Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.2(1)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Sun 27-Nov-11 21:19 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2011 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

ROM: IOS-XE ROMMON
```

Router uptime is 1 minute
Uptime for this control processor is 3 minutes
System returned to ROM by reload
System restarted at 22:07:05 UTC Sun Nov 27 2011
System image file is "tftp:/auto/tftp-smoke2/mcpdt-rp2-14/vmlinux"
Last reload reason: PowerOn

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

If you require further assistance please contact us by sending email to export@cisco.com.

cisco ASR1006 (RP2) processor with 4252282K/6147K bytes of memory.
5 Gigabit Ethernet interfaces
2 Channelized T3 ports
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
192519K bytes of eUSB flash at bootflash:.
78085207K bytes of SATA hard disk at harddisk:.

Configuration register is 0x2102
Determining the Individual Subpackages Installed

To determine the version of the individual subpackages running on your Cisco ASR 1000 Series Router, log in to the router and enter the `show version installed` command in the User EXEC, Privileged EXEC, or Diagnostic mode.

The following is sample output of the `show version installed` command. The actual output displayed when you run the command will vary depending on the version of the product that you are using.

```
Router# show version installed

Package: Provisioning File, version: n/a, status: active
  File: consolidated:packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: 96de495067ade7bb7e17f833fb3e41364ddff0a7

Package: rpbase, version: 03.05.00.S.152-1.S, status: active
  File: consolidated:asr1000rp2-rpbase.03.05.00.S.152-1.S.pkg, on: RP0
  Built: 2011-11-27_15.35, by: mcpre
  File SHA1 checksum: aadf1bfa5ff97720c3eeaed32e4d9941e54b0ea8

Package: rpcontrol, version: 03.05.00.S.152-1.S, status: active
  File: consolidated:asr1000rp2-rpcontrol.03.05.00.S.152-1.S.pkg, on: RP0/0
  Built: 2011-11-27_15.41, by: mcpre
  File SHA1 checksum: 57f1f2c5536098d761d228d3a4d5031bf1f885fb

Package: rpios-adventerprisek9, version: 03.05.00.S.152-1.S, status: active
  File: consolidated:asr1000rp2-rpios-adventerprisek9.03.05.00.S.152-1.S.pkg, on: RP0/0
  Built: 2011-11-27_15.41, by: mcpre
  File SHA1 checksum: 632836be203f1f5a94d7cbb4eb042890649d5b0d

Package: rpaccess, version: 03.05.00.S.152-1.S, status: active
  File: consolidated:asr1000rp2-rpaccess.03.05.00.S.152-1.S.pkg, on: RP0/0
  Built: 2011-11-27_15.35, by: mcpre
  File SHA1 checksum: adc4045026a793a1523431f108806b6bf1fa1fb2c

Package: rpcontrol, version: 03.05.00.S.152-1.S, status: n/a
  File: consolidated:asr1000rp2-rpcontrol.03.05.00.S.152-1.S.pkg, on: RP0/1
  Built: 2011-11-27_15.35, by: mcpre
  File SHA1 checksum: 57f1f2c5536098d761d228d3a4d5031bf1f885fb

Package: rpios-adventerprisek9, version: 03.05.00.S.152-1.S, status: n/a
  File: consolidated:asr1000rp2-rpios-adventerprisek9.03.05.00.S.152-1.S.pkg, on: RP0/1
  Built: 2011-11-27_15.41, by: mcpre
  File SHA1 checksum: 632836be203f1f5a94d7cbb4eb042890649d5b0d

Package: rpaccess, version: 03.05.00.S.152-1.S, status: n/a
  File: consolidated:asr1000rp2-rpaccess.03.05.00.S.152-1.S.pkg, on: RP0/1
  Built: 2011-11-27_15.35, by: mcpre
  File SHA1 checksum: adc4045026a793a1523431f108806b6bf1fa1fb2c

Package: rpbase, version: 03.05.00.S.152-1.S, status: n/a
  File: consolidated:asr1000rp2-rpbase.03.05.00.S.152-1.S.pkg, on: RP1
  Built: 2011-11-27_15.35, by: mcpre
  File SHA1 checksum: aadf1bfa5ff97720c3eeaed32e4d9941e54b0ea8

Package: rpcontrol, version: 03.05.00.S.152-1.S, status: n/a
  File: consolidated:asr1000rp2-rpcontrol.03.05.00.S.152-1.S.pkg, on: RP1/0
  Built: 2011-11-27_15.35, by: mcpre
  File SHA1 checksum: 57f1f2c5536098d761d228d3a4d5031bf1f885fb

Package: rpios-adventerprisek9, version: 03.05.00.S.152-1.S, status: n/a
  File: consolidated:asr1000rp2-rpios-adventerprisek9.03.05.00.S.152-1.S.pkg, on: RP1/0
```
Determining the Software Version

Built: 2011-11-27_15.41, by: mcpre
File SHA1 checksum: 632836be203f1f5a94d7cbb4eb042890649d5b0d

Package: rpaccess, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-rpaccess.03.05.00.S.152-1.S.pkg, on: RP1/0
Built: 2011-11-27_15.35, by: mcpre
File SHA1 checksum: adc4045026a793a152343f1f10860b6bf1fa1fb2c

Package: rpcontrol, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-rpcontrol.03.05.00.S.152-1.S.pkg, on: RP1/1
Built: 2011-11-27_15.35, by: mcpre
File SHA1 checksum: 57f1f2c5536098d761d2283da45031bf1ff885fb

Package: rpios-adventerprisek9, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-rpios-adventerprisek9.03.05.00.S.152-1.S.pkg, on: RP1/1
Built: 2011-11-27_15.41, by: mcpre
File SHA1 checksum: adc4045026a793a152343f1f10860b6bf1fa1fb2c

Package: espbase, version: 03.05.00.S.152-1.S, status: active
File: consolidated:asr1000rp2-espbase.03.05.00.S.152-1.S.pkg, on: ESP0
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 686fbb534e17b884c5859175ad70891c49f05

Package: espx86base, version: 03.05.00.S.152-1.S, status: inactive
File: consolidated:asr1000rp2-espx86base.03.05.00.S.152-1.S.pkg, on: ESP0
Built: 2011-11-27_15.35, by: mcpre
File SHA1 checksum: 6d11715ea722191f66de8bec077512fd22c473ae

Package: espx86base, version: 03.05.00.S.152-1.S, status: inactive
File: consolidated:asr1000rp2-espx86base.03.05.00.S.152-1.S.pkg, on: ESP1
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 686fbb534e17b884c5859175ad70891c49f05

Package: sipbase, version: 03.05.00.S.152-1.S, status: active
File: consolidated:asr1000rp2-sipbase.03.05.00.S.152-1.S.pkg, on: SIP0
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 216029d6fb614f3b65225015008d25e70b513169

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP0/0
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP0/1
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipspa, version: 03.05.00.S.152-1.S, status: active
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP0/2
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipspa, version: 03.05.00.S.152-1.S, status: active
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP0/3
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipbase, version: 03.05.00.S.152-1.S, status: active
File: consolidated:asr1000rp2-sipbase.03.05.00.S.152-1.S.pkg, on: SIP1
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 216029d6fb614f3b65225015008d25e70b513169

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP1/0
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP1/1
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP1/2
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipbase, version: 03.05.00.S.152-1.S, status: active
File: consolidated:asr1000rp2-sipbase.03.05.00.S.152-1.S.pkg, on: SIP1/3
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP2/0
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP2/1
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP2/2
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP2/3
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipbase, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipbase.03.05.00.S.152-1.S.pkg, on: SIP3
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 216029d6fb614f3b65225015008d25e70b513169

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP3/0
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5
Determining the Software Version

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP3/1
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP3/2
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP3/3
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipbase, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipbase.03.05.00.S.152-1.S.pkg, on: SIP4
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 216029d6fb614f3b65225015008d25e70b513169

Package: sipspa, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipspa.03.05.00.S.152-1.S.pkg, on: SIP4/0
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 58250807ef37ef9da6c3952babce9a9a5b5e29b5

Package: sipbase, version: 03.05.00.S.152-1.S, status: n/a
File: consolidated:asr1000rp2-sipbase.03.05.00.S.152-1.S.pkg, on: SIP5
Built: 2011-11-27_15.14, by: mcpre
File SHA1 checksum: 216029d6fb614f3b65225015008d25e70b513169
Cisco IOS XE 3S to Cisco IOS Version Number Mapping

Each version of Cisco IOS XE 3S has an associated Cisco IOS version. Table 6 lists these mappings for all released versions of Cisco IOS XE 3S.

<table>
<thead>
<tr>
<th>Cisco IOS XE 3S Version</th>
<th>Cisco IOS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.0S</td>
<td>15.0(1)S</td>
</tr>
<tr>
<td>3.1.1S</td>
<td>15.0(1)S1</td>
</tr>
<tr>
<td>3.1.2S</td>
<td>15.0(1)S2</td>
</tr>
<tr>
<td>3.1.3S</td>
<td>15.0(1)S3</td>
</tr>
<tr>
<td>3.1.4S</td>
<td>15.0(1)S4</td>
</tr>
<tr>
<td>3.1.4aS</td>
<td>15.0(1)S4a</td>
</tr>
<tr>
<td>3.2.0S</td>
<td>15.1(1)S</td>
</tr>
<tr>
<td>3.2.1S</td>
<td>15.1(1)S1</td>
</tr>
<tr>
<td>3.2.2S</td>
<td>15.1(1)S2</td>
</tr>
<tr>
<td>3.3.0S</td>
<td>15.1(2)S</td>
</tr>
<tr>
<td>3.3.1S</td>
<td>15.1(2)S1</td>
</tr>
<tr>
<td>3.3.2S</td>
<td>15.1(2)S2</td>
</tr>
<tr>
<td>3.4.0S</td>
<td>15.1(3)S</td>
</tr>
<tr>
<td>3.4.0aS</td>
<td>15.1(3)S0a</td>
</tr>
<tr>
<td>3.4.1S</td>
<td>15.1(3)S1</td>
</tr>
<tr>
<td>3.4.2S</td>
<td>15.1(3)S2</td>
</tr>
<tr>
<td>3.4.3S</td>
<td>15.1(3)S3</td>
</tr>
<tr>
<td>3.4.4S</td>
<td>15.1(3)S4</td>
</tr>
<tr>
<td>3.4.5S</td>
<td>15.1(3)S5</td>
</tr>
<tr>
<td>3.4.6S</td>
<td>15.1(3)S6</td>
</tr>
<tr>
<td>3.5.0S</td>
<td>15.2(1)S</td>
</tr>
<tr>
<td>3.5.1S</td>
<td>15.2(1)S1</td>
</tr>
<tr>
<td>3.5.2S</td>
<td>15.2(1)S2</td>
</tr>
</tbody>
</table>

Upgrading to a New Software Release

Only Cisco IOS XE 3S consolidated packages can be downloaded from Cisco.com; users who want to run the router using individual subpackages must first download the image from Cisco.com and extract the individual subpackages from the consolidated package.

For information about upgrading to a new software release, see Cisco ASR 1000 Series Aggregation Services Router Software Configuration Guide at the following location:
Limitations and Restrictions in Cisco IOS XE 3S Releases

This chapter describes the limitations and restrictions applicable to the Cisco ASR 1000 Series Routers and Cisco ASR 903 Series Router for Cisco IOS XE 3S releases:

- Limitations and Restrictions in Cisco IOS XE Release 3.5.2S, page 36
- Limitations and Restrictions in Cisco IOS XE Release 3.5.1S, page 36
- Limitations and Restrictions in Cisco IOS XE Release 3.5.0S, page 37
- Limitations and Restrictions in Cisco IOS XE Release 3.4.6S, page 39
- Limitations and Restrictions in Cisco IOS XE Release 3.4.5S, page 39
- Limitations and Restrictions in Cisco IOS XE Release 3.4.4S, page 39
- Limitations and Restrictions in Cisco IOS XE Release 3.4.3S, page 39
- Limitations and Restrictions in Cisco IOS XE Release 3.4.2S, page 39
- Limitations and Restrictions in Cisco IOS XE Release 3.4.1S, page 39
- Limitations and Restrictions in Cisco IOS XE Release 3.4.0aS, page 40
- Limitations and Restrictions in Cisco IOS XE Release 3.4.0S, page 40
- Limitations and Restrictions in Cisco IOS XE Release 3.3.2S, page 41
- Limitations and Restrictions in Cisco IOS XE Release 3.3.1S, page 41
- Limitations and Restrictions in Cisco IOS XE Release 3.3.0S, page 41
- Limitations and Restrictions in Cisco IOS XE Release 3.2.2S, page 42
- Limitations and Restrictions in Cisco IOS XE Release 3.2.1S, page 42
- Limitations and Restrictions in Cisco IOS XE Release 3.2.0S, page 42
- Limitations and Restrictions in Cisco IOS XE Release 3.1.4aS, page 43
- Limitations and Restrictions in Cisco IOS XE Release 3.1.4S, page 43
- Limitations and Restrictions in Cisco IOS XE Release 3.1.3S, page 44
- Limitations and Restrictions in Cisco IOS XE Release 3.1.2S, page 44
- Limitations and Restrictions in Cisco IOS XE Release 3.1.1S, page 44
Limitations and Restrictions in Cisco IOS XE Release 3.5.2S

There are no new limitations and restrictions in Cisco IOS XE Release 3.5.2S.

Limitations and Restrictions in Cisco IOS XE Release 3.5.1S

This section describes limitations and restrictions in Cisco IOS XE Release 3.5.1S and later releases.

Multi-Segment Pseudowire Limitation

- The Cisco ASR 903 Series Router does not support l2vpn Inter-AS.
- VCCV type RA (Router Alert) is not supported with Multi-Segment Pseudowire.
- Multi-Segment Pseudowires are supported only on EVC service instances, as in the following configuration in which the Cisco ASR 903 Series Router acts as the terminating PE (T-PE) router.

```plaintext
interface TenGigabitEthernet2/0/0
no ip address
no mls qos trust
service instance 2001 ethernet
encapsulation dot1q 2001
rewrite ingress tag pop 1 symmetric
xconnect 1.1.1.1 2001 encapsulation mpls
```

QoS ACL Restrictions

- QoS ACLs are supported only for IPv4 traffic.
- QoS ACLs are supported only for ingress traffic.
- You can use QoS ACLs to classify traffic based on the following criteria:
  - Source and destination host
  - Source and destination subnet
  - TCP source and destination
  - UDP source and destination
- Named and numbered ACLs are supported.
- You can apply QoS ACLs only to the third level class (bottom-most).
- The following range of numbered access lists are supported:
Limitations and Restrictions in Cisco IOS XE Release 3.5.0S

You must create an ACL before referencing it within a QoS policy.
• Deny statements within an ACL are ignored for the purposes of classification.
• Classifying traffic based on TCP flags using an ACL is not supported.
• Classifying traffic using multiple mutually exclusive ACLs within a match-all class-map is not supported.
• Classifying traffic on a logical/physical level using an ACL is not supported.
• Applying QoS ACLs to MAC addresses is not supported.
• The `neq` keyword is not supported with the `access-list permit` and `ip access-list extended` commands.
• This release does not support matching on multiple port numbers in a single ACE, as in the following command: `permit tcp any eq 23 45 80 any`

Resilient Ethernet Protocol Limitations

• Resilient Ethernet Protocol (REP) is supported only on trunk EFP interfaces.
• The `ethernet vlan color-block` command is not supported.
• REP is not supported on cross-connect and local connect EVCs.
• REP is not supported on port-channel interfaces.

Limitations and Restrictions in Cisco IOS XE Release 3.5.0S

This section describes limitations and restrictions in Cisco IOS XE Release 3.5.0S and later releases.

ATM IMA Limitation

You can create a maximum of 16 IMA groups on each T1/E1 interface module.

Clocking and Timing Limitation

Only a single clocking input source can be configured within each group of eight ports (0-7 and 8-15) on the T1/E1 interface module using the `network-clock input-source` command.

Ethernet IM Restrictions

• The Cisco ASR 903 Series Router does not support the Facilities Data Link (FDL) on Ethernet interfaces.
- The Cisco ASR 903 Series Router does not support the `mac-address` command on Gigabit Ethernet interface modules.
- On the Cisco ASR 903 Series Router, 10 Gigabit Ethernet interface modules are not supported in slots 4 and 5.
- When you install a Gigabit Ethernet IM in slot 5, the interface GigabitEthernet0/5/0 is not operational; the port is reserved for internal communication.

**Pseudowire/AToM Limitation**

Cisco IOS Release 15.2(1)S does not support ATM over MPLS N-to-one cell mode or one-to-one cell mode.

**QoS Limitations**

- QoS policies are not supported on Link Aggregation (LAG) bundle interfaces or port-channel interfaces configured with Ethernet Flow Points (EFPs).
- QoS policies are not supported on physical interfaces configured with an EFP.
- The Cisco ASR 903 Series Router supports up to 64 unique QoS classification service instances in a given bridge domain. QoS service instances refer to ports, VLAN classes, and EFPs associated with a QoS classification policy.
- Modification of policy-map and class-map definitions while applied to an interface or EFP is not supported.
- Policy validation—Some QoS policy configurations are not validated until you apply the policy-map to an interface or EFP.
- If a QoS configuration is invalid, the router rejects the configuration when you apply it to an interface. In some cases, a QoS configuration may be rejected due to hardware resource exhaustion or limitations. If you receive such an error message, detach the policy and adjust your QoS configuration.
- The `match-all` keyword is supported only for QinQ classification.
- QoS is not supported on Time Division Multiplexing (TDM) interfaces.
- The class-based QoS MIB is not supported.

**Subinterfaces Limitation**

The Cisco ASR 903 router does not support subinterface configurations in Cisco IOS XE Release 3.5.0S.

**T1/E1 IM Limitations**

- Serial interfaces are not supported—The current software release does not support serial interfaces or features applied to serial interfaces. It is recommended that you use a configuration with circuit emulation (CEM) or Inverse Multiplexing over ATM (ATM IMA) as a workaround.
- Channel groups is not supported—The current software release does not support configuration of an EtherChannel group using the `channel-group interface` command.
IP addresses are not supported—The current software release does not support specifying an IP address on a T1/E1 interface. You can specify an address on the interface by configuring it as a part of a CEM group using the `cem-group` command or as a part of an ATM IMA `ima-group` command. For more details, see the Cisco ASR 903 Series Aggregation Services Router Chassis Software Configuration Guide.

- Configuring encapsulation is not supported—The current software release does not support configuration of Layer 2 encapsulation using the `encapsulation interface` command.
- T1/E1 CRC size is not supported—The current software release does not support configuration of a T1 or E1 CRC size using the `crc` command.
- Inverting data on the T1/E1 interface is not supported—Inverting the data stream using the `invert data interface` command is not supported.
- Bit error rate test (BERT) patterns have limited support—Currently, only the $2^{11}$, $2^{15}$, $2^{20}$-O153, and $2^{20}$-QRSS patterns are supported for BERT.

Limitations and Restrictions in Cisco IOS XE Release 3.4.6S

There are no new limitations and restrictions in Cisco IOS XE Release 3.4.6S.

Limitations and Restrictions in Cisco IOS XE Release 3.4.5S

There are no new limitations and restrictions in Cisco IOS XE Release 3.4.5S.

Limitations and Restrictions in Cisco IOS XE Release 3.4.4S

There are no new limitations and restrictions in Cisco IOS XE Release 3.4.4S.

Limitations and Restrictions in Cisco IOS XE Release 3.4.3S

There are no new limitations and restrictions in Cisco IOS XE Release 3.4.3S.

Limitations and Restrictions in Cisco IOS XE Release 3.4.2S

There are no new limitations and restrictions in Cisco IOS XE Release 3.4.2S.

Limitations and Restrictions in Cisco IOS XE Release 3.4.1S

This section describes limitations and restrictions in Cisco IOS XE Release 3.4.1S and later releases.
sVTI and GRE Tunnel Protection Limitation

The limitations and restrictions on sVTI and GRE tunnel protection in Cisco IOS XE Release 3.4.1S are as follows:

- When using static VTI-based IPSec on a Cisco ASR 1000 Router, if there are multiple remote IPSec endpoints behind the same NAT device, their peer sVTI tunnels must not share the same tunnel source and tunnel destination addresses.
- When using GRE tunnel protection on a Cisco ASR 1000 Router, if there are multiple remote IPSec endpoints behind the same NAT device, their peer GRE Tunnel protection tunnels must not share the same tunnel source and tunnel destination addresses, at the same time, the IPSec mode must be set to transport mode when configuring the corresponding IPSec transform-set.

Limitations and Restrictions in Cisco IOS XE Release 3.4.0aS

There are no new limitations and restrictions in Cisco IOS XE Release 3.4.0aS.

Limitations and Restrictions in Cisco IOS XE Release 3.4.0S

The limitations and restrictions for using SPA-24CHT1-CE-ATM in Cisco IOS XE Release 3.4.0S are as follows:

- The SPA-24CHT1-CE-ATM is not supported on the Cisco ASR 1001 Router (1 RU chassis), but supported on all other ASR 1000 chassis.
- The SPA-24CHT1-CE-ATM supports only the CEM mode and not the ATM in Cisco IOS XE Release 3.4.0S.
- The SPA-24CHT1-CE-ATM is supported on Cisco IOS XE Release 3.4.0S and later releases only with these software images: ADVANCED ENTERPRISE SERVICES, ADVANCED ENTERPRISE W/O CRYPTO, ADVANCED IP SERVICES, or ADVANCED IP SERVICES W/O CRYPTO.
- The SPA-24CHT1-CE-ATM is not supported with these software images: IP BASE and IP BASE W/O CRYPTO.
- SPA-24CHT1-CE-ATM does not support ATM and IMA.
- CESoPSN over L2TPv3 is not supported.
- SAToP over L2TPv3 is not supported.
- CEM Access Circuit Redundancy is not supported.

The limitations and restrictions for using SPA-2CHT3-CE-ATM in Cisco IOS XE Release 3.4.0 are as follows:

- The SPA-2CHT3-CE-ATM is supported on Cisco IOS XE Release 3.4.0S and later releases.
- The SPA-2CHT3-CE-ATM is not supported on the Cisco ASR 1001 Router (1 RU chassis), but supported on all other ASR 1000 chassis.
  However, the SPA-2CHT3-CE-ATM supports only the ATM mode in Cisco IOS XE Release 3.4.0 and not the Circuit Emulation (CEM) mode.
- Maximum virtual circuits: 1,000
- Per-virtual circuit and per-virtual path traffic shaping is not supported.
• Switched virtual circuits (SVCs) is not supported.
• Interim Local Management Interface (ILMI) 1.0 is not supported.
• IETF RFC 2364 and 2516 for Point-to-Point Protocol (PPP) over ATM is not supported.
• IETF RFC 1577 support for classical IP and Address Resolution Protocol (ARP) over ATM is not supported.
• ATM Forum UNI 3.0, 3.1, and 4.0 is not supported.
• SPA-2CHT3-CE-ATM SPA does not support port channelization for ATM.
• NLPID encapsulation type is not supported.
• Maximum virtual circuits supported are 1,000.
• The SPA-2CHT3-CE-ATM does not support the CBIT Physical Layer Convergence Protocol (PLCP) framing.
• Only the Clear T3 mode is supported.
• The IMA mode is not supported on SPA-2CHT3-CE-ATM CEoP in Cisco IOS XE Release 3.4.0.
• POS and HDLC capabilities are not supported.
• Inverse Multiplexing over ATM (IMA) is not supported.
• ATM Local Switching is not supported.

The limitations and restrictions for using RTCP service on SPA-DSP in the Cisco IOS XE Release 3.4.0 are as follows:
• The length of the CNAME in the RTCP packets sent by endpoints should not exceed 40 bytes.
• If one endpoint does not send the RTP packets, the SPA-DSP neither generates the RTCP packets nor sends the RTCP packets to the other side.

The following is a limitation related to configuring an IPv6 over IPv4 GRE tunnel:
• In the context of an IPv6 over IPv4 GRE tunnel, if you want to configure the keepalive feature, an IPv4 address must be configured on the tunnel.

Limitations and Restrictions in Cisco IOS XE Release 3.3.2S

There are no new limitations and restrictions in Cisco IOS XE Release 3.3.2S.

Limitations and Restrictions in Cisco IOS XE Release 3.3.1S

There are no new limitations and restrictions in Cisco IOS XE Release 3.3.1S.

Limitations and Restrictions in Cisco IOS XE Release 3.3.0S

The following are the limitations and restrictions in Cisco IOS XE Release 3.3.0S and later releases:
• The SPA-1CHOC3-CE-ATM is not supported on the Cisco ASR 1001 Router, but is supported on all the other Cisco ASR 1000 Series Routers.
• All the other ASR 1000 Routers support the SPA-1CHOC3-CE-ATM for Circuit Emulation applications, but not ATM applications.

The limitations and restrictions for using RTCP service on SPA-DSP in the Cisco IOS XE Release 3.4.0 are as follows:
• The length of the CNAME in the RTCP packets sent by endpoints should not exceed 40 bytes.
• If one endpoint does not send the RTP packets, the SPA-DSP neither generates the RTCP packets nor sends the RTCP packets to the other side.

The following is a limitation related to configuring an IPv6 over IPv4 GRE tunnel:
• In the context of an IPv6 over IPv4 GRE tunnel, if you want to configure the keepalive feature, an IPv4 address must be configured on the tunnel.
• The SPA-1CHO3-CE-ATM is supported on Cisco IOS XE Release 3.3.0S and later releases only with these software images: ADVANCED ENTERPRISE SERVICES, ADVANCED ENTERPRISE W/O CRYPTO, ADVANCED IP SERVICES, and ADVANCED IP SERVICES W/O CRYPTO.

• The SPA-1CHO3-CE-ATM is not supported with these software images: IP BASE and IP BASE W/O CRYPTO.

Limitations and Restrictions in Cisco IOS XE Release 3.2.2S

There are no new limitations and restrictions in Cisco IOS XE Release 3.2.2S.

Limitations and Restrictions in Cisco IOS XE Release 3.2.1S

The following are the limitations and restrictions in Cisco IOS XE Release 3.2.1S and later releases:

• On the standby RP, auto service level-initiated sessions containing IPv6 ACLs do not follow the template. This condition is observed consistently in the context of ACLs that can follow IPv6 templates. As a workaround, you can use the user level setting per-user avpair to define ACLs externally.
  However, IPv4-initiated sessions with the auto service level setting follow the template correctly.

• An IPv6 traffic filter cannot be configured under the policy map type service. Due to this, Service Logon profiles cannot be defined locally. As a workaround, you can use RADIUS to define Service Logon profiles.

Limitations and Restrictions in Cisco IOS XE Release 3.2.0S

This section describes limitations and restrictions in Cisco IOS XE Release 3.2.0S and later releases.

IPSec on Cisco ASR 1000 Routers

The following limitations and restrictions are related to the use of IPSec on Cisco ASR 1000 Routers:

• In the context of an IPSec DVTI Connection, the Cisco ASR 1000 Router does not support dynamic download ACL rule (per-user attribute) from the AAA server.
  For example, the following configurations are not supported:
  cisco-avpair += "ip:inacl#1=permit ip any 2.2.2.0 0.0.0.255"
  cisco-avpair += "ip:outacl#1=permit ip 2.2.2.0 0.0.0.255 any"

• The Cisco ASR 1000 Router does not support the if-state nhrp command in configuring the tunnel.

• The Cisco ASR 1000 Router Dead Peer Detection behavior is different than the pre-defined behavior (i.e. when there is no traffic to be sent, no DPD is sent, while if any traffic to be sent, DPD is sent). A Cisco ASR 1000 Router DPD is sent out regardless there is outbound traffic needs to be sent out.

• The Cisco ASR 1000 Router does not support SA Path MTU on data path.

• The Cisco ASR 1000 Router does not support double ACL in dynamic crypto map.
• VRF without crypto map configured on a physical interface causes dual esp reload on a Cisco ASR 1000 Router.

• The command: `show crypto ipsec sa identity` does not log send and receive error counts.

• The commands: `clear crypto` and `show crypto` on Standby RP are inconsistent with Active RP. At present most of other features disable 'clear commands' from Standby RP, but IPSec still allows to clear sa, session etc. from the standby.

• The Cisco ASR 1000 Router does not support Cisco AAA av-pair “cisco-avpair += ip:sub-policy-In=policy1”.

• CLI allows both ikev1 and ikev2 profile configured under the same crypto map, even though it is not supported internally on the ASR 1000 Router.

• For a Cisco ASR 1000 Router, the tunnel protection should be removed first before changing any configuration for tunnel protection.

• On a Cisco ASR 1000 Router, when an EzVPN session is ended, the EzVPN server sends out the STOP accounting message. This message does not contain the Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, and Acct-Output-Packets fields. It might cause a disruption in the accounting process.

• When using dynamic VTI-based IPSec on a Cisco ASR 1000 Router, if there are multiple remote IPSec endpoints behind the same NAT device, only one of the endpoints has connectivity. In other words, multiple endpoints cannot have connectivity at the same time.

TCP Failover in the Hardware High-Availability Mode

TCP failover is not supported in the Hardware High Availability mode. If the active node fails in the Hardware High Availability mode and if the network is then restored, it may take 5 to 10 minutes for the standby node to become the active node. This is because of the reboot and the peer negotiation delay. If the network is not restored, only the switched-over active peer is available. Failover is not possible in this state.

Tunneling on Cisco ASR 1000 Routers

The Cisco ASR 1000 Router does not support multi-VRF selection by the PBR feature on the tunnel interfaces on which the `ip vrf receive` setting has been configured.

Limitations and Restrictions in Cisco IOS XE Release 3.1.4aS

There are no new limitations and restrictions in Cisco IOS XE Release 3.1.4aS.

Limitations and Restrictions in Cisco IOS XE Release 3.1.4S

There are no new limitations and restrictions in Cisco IOS XE Release 3.1.4S.
Limitations and Restrictions in Cisco IOS XE Release 3.1.3S

There are no new limitations and restrictions in Cisco IOS XE Release 3.1.3S.

Limitations and Restrictions in Cisco IOS XE Release 3.1.2S

There are no new limitations and restrictions in Cisco IOS XE Release 3.1.2S.

Limitations and Restrictions in Cisco IOS XE Release 3.1.1S

This section describes the limitations and restrictions in Cisco IOS XE Release 3.1.1S and later releases.

Flexible NetFlow (FNF)

This section describes limits and restrictions related to Cisco Flexible Netflow features in Cisco IOS XE Release 3.1.1S on the Cisco ASR 1000 Series Router.

- V5 (old style) export with any user-defined flow record format is not supported. This applies even when the user-defined format is a subset of a supported v5 format. For more details, see CSCti69232.
- NetFlow on BB sessions is not supported. For more details, see CSCsx24985.

Note

CSCsx24985 applies to both Cisco tNF and Cisco FNF features.

- v6 FNF is not supported. For more details, see CSCsx24985.
- MPLS netflow is not supported. For more details, see CSCtf39723.
- FNF ISSU/SSO is not supported. For more details, see CSCth71187.

For more information, see Cisco IOS XE Flexible NetFlow Overview at the following location: http://www.cisco.com/en/US/docs/ios/ios_xe/fnetflow/configuration/guide/fnetflow_overview_xe.html

Limitations and Restrictions in Cisco IOS XE Release 3.1.0S

This section describes limitations and restrictions in Cisco IOS XE Release 3.1.0S and later releases.

SIP-40G:SPA-4XT-SERIAL

SIP-40G:SPA-4XT-SERIAL was not supported in Release 3.1.0S when plugged into a Cisco ASR1000 Series Router with SIP-40 linecard. This SPA is supported in Release 3.1.1S on a SIP-40 linecard.
**FNF**

The Cisco FNF feature is not supported in Cisco IOS XE Release 3.1.0S on the Cisco ASR 1000 Series Router.

**SDH support on 1xCHOC12/DS0 SPA**

SDH framing is not supported in Cisco IOS XE Release 3.1.0S for the 1xCHOC12/DS0 SPA. SONET is the only supported in framing mode. SDH framing support will be supported, starting in Cisco IOS XE Release 3.1.1S on 1xCHOC12/DS0 SPA.

**uRPF ACL**

The Cisco ASR 1000 Series Routers do not support uRPF ACL.

**Interchassis and Intrachassis Support**

Coexistence of interchassis high availability and intrachassis high availability is not supported. In the Cisco ASR 1001 Router, Cisco ASR 1002 Router, and Cisco ASR 1004 Router, interchassis redundancy is not supported with software redundancy. In the Cisco ASR 1006 Router and Cisco ASR 1013 Router, interchassis redundancy is not supported with intrachassis redundancy. It is supported with only a single RP and ESP in the chassis.

**GRE Keepalive with Tunnel Protection**

The Cisco ASR 1000 Series Router supports GRE keepalive with tunnel protection. However, the keepalive packet that is returned is not encrypted.

**Limitations and Restrictions in Cisco IOS XE Release 2.3.0**

This section describes limitations and restrictions in Cisco IOS XE Release 2.3.0 and later releases.

**User-Defined Parent Class Limitation (for Hierarchical QoS)**

On a Cisco ASR 1000 Series Router with hierarchical QoS and user-defined parent classes applied, each child policy must be a unique policy map. The use of a single child policy map in multiple instances in the definition of a user-defined parent class is not supported in Cisco IOS XE Release 2.3.0. For more details, see CSCsr56079.
Limitations and Restrictions in Cisco IOS XE Release 2.2.3

User-Defined Parent Class Limitation (for Conditional Policer)

On a Cisco ASR 1000 Series Router with hierarchical QoS and user-defined parent classes applied, each child policy must use an unconditional policer (priority + policer). The use of conditional policers (priority x kbps) is not supported in these configurations in Cisco IOS XE Release 2.3.0. For more details, see CSCsy99583.

Deny ACL Limitation for GET VPN

No more than 8 deny access control lists (ACLs) (a total of Key Server downloaded and group member local) are supported for Group Encrypted Transport VPN (GET VPN) in Cisco IOS XE Release 2.3.0. For more details, see CSCsy24144.

Limitation Related to the Use of Deny Statements in QoS Classification

Large numbers of deny statements should not be used as access control entries (ACEs) in access control lists (ACLs) used for Quality of Service (QoS) classification in Cisco IOS XE Release 2.3.0. The number of deny statements and the order of these statements with other permit statements in an ACL determines the amount of content-addressable memory (TCAM) used, and there is no fixed number quantified as a limit for this configuration. For more details, see CSCsx16234.

Limitations and Restrictions in Cisco IOS XE Release 2.2.3

This section describes limitations and restrictions in Cisco IOS XE Release 2.2.3 and later releases.

DMVPN Limitation

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. When this condition occurs, perform shut/no shut on the specific spoke for which the hub does not have the entry in the hardware.

Scaling Limits for MLP

The supported scaling limits for Multilink PPP (MLP) for Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2.3 and later releases are as follows:

- 123 10-link bundles
• 245 5-link bundles
• 616 2-link bundles

The maximum scaling limit for LFI is 1232 single-link bundles.

If either the maximum number of bundles or maximum number of links are exceeded, the interface line rate may not be maintained. This limitation is especially applicable for configurations that have a high number of links per bundle and a high number of features enabled.

Limitations and Restrictions in Cisco IOS XE Release 2.2.1

This section describes limitations and restrictions in Cisco IOS XE Release 2.2.1 and later releases.

Cisco Firewall and WAAS Inter-Op Limitations and Restrictions

The Cisco Firewall and WAAS Interoperability feature is subject to the following limitations and restrictions in Cisco IOS XE Release 2.2.1:

• Only Generic Routing Encapsulation (GRE) redirect and return is supported. Layer 2 redirect and return is not supported.
• Certain platforms, such as the Cisco 2800 series, support an inbox network service module (WAAS-NM) that provides WAAS services. The Cisco ASR 1000 Series Routers do not support inbox network service modules; thus, the router will not support WAAS-NM.

Control Plane Policing (CoPP) Limitations and Restrictions

Control Plane Policing (CoPP) does not support match protocol l2tp and match protocol dhcp for Cisco IOS XE Release 2.2.1. However, because CoPP supports packet matching with access lists, you can police Layer 2.

L2TP and DHCP packets can be matched by access lists. For example, L2TP and DHCP packets can be matched with access lists that check UDP packet port number (1701 for L2TP, 67 and 68 for DHCP).

Flexible Packet Matching (FPM) Limitations and Restrictions

Flexible Packet Matching (FPM) support is subject to the following limitations and restrictions in Cisco IOS XE Release 2.2.1:
• Table 1 describes the functionality supported in the Raw FPM and Basic FPM (Raw FPM+) modes in Cisco IOS XE Release 2.2.1.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Supported Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw FPM</td>
<td>• Supports Raw offset and bit pattern matching from L2 or L3 start</td>
</tr>
<tr>
<td></td>
<td>• Protocol unaware</td>
</tr>
<tr>
<td></td>
<td>• Match string pattern up to 32 bytes</td>
</tr>
<tr>
<td></td>
<td>• Regular expression matching</td>
</tr>
<tr>
<td></td>
<td>• Packet inspection depth: 256 bytes</td>
</tr>
<tr>
<td></td>
<td>• Maximum 32 classes are supported in a policy-map; 8 entries per class map</td>
</tr>
<tr>
<td>Basic FPM (Raw FPM+)</td>
<td>• PHDF nomenclature (for fixed length fields)</td>
</tr>
<tr>
<td></td>
<td>• Support for building protocol stacks (for static header length only)</td>
</tr>
</tbody>
</table>

• Although Cisco IOS XE Release 2.2.1 does not support the traffic classification description file (TCDF), bittorrent, iis-unicode, ios-http-vuln and skype can be configured manually.

L2TP AAA Accounting Include NAS-PORT (VPI/VCI) Limitation

In Cisco IOS XE Release 2.2.1, the L2TP AAA Accounting Include NAS-PORT feature does not support the asynchronous transfer mode (ATM) virtual path identifier/virtual channel identifier (VPI/VCI) pair.

Limitations and Restrictions in Cisco IOS XE Release 2.1.1

This section describes the limitations and restrictions in Cisco IOS XE Release 2.1.1 and later releases.

Maximum Number of Broadband Tunnels Limitation

Up to 16K broadband tunnels are supported in Cisco IOS XE Release 2.1.1.

Maximum Number of IPSec Tunnels Limitation

Up to 4K IPSec tunnels are supported in Cisco IOS XE Release 2.1.1.

Limitations and Restrictions in Cisco IOS XE Release 2.1.0

This section describes limitations and restrictions in Cisco IOS XE Release 2.1.0 and later releases.
IPv6 Source Address of ICMPv6 Error Message

Note
This limitation has been removed in Release 3.4.0 and later releases.

When all the interface related to ICMPv6 error message generation or forwarding have only the IPv6 link-local address in place, link-local is set as the source address of generation ICMPv6 error messages.

The interface types related to ICMPv6 error message generation or forwarding are:
1. The interface by which the original packet is received. The original packet refers to the packet triggering the ICMPv6 error message.
2. The interface by which the original packet should be sent out there is no incident to trigger an ICMPv6 error message.
3. The interface by which the ICMPv6 error message is sent out. To perform asymmetric routing, the interfaces described in the pervious items are different, otherwise, the interfaces are identical.

IPv6 Address Support on ASR1000 Hardware Interfaces

On the Cisco ASR 1000 Series Router, only one IPv6 IP address exists for each interface. Even if, several IPv6 IP addresses are configured on an interface, only the lowest IPv6 IP address is downloaded to the hardware.

The Cisco ASR 1000 Router hardware, supports only one IPv6 address for each interface. Therefore, even if several IPv6 IP addresses are configured on an interface, in Cisco IOS, only the lowest IPv6 address is downloaded to the hardware.

Note
When IPv6 is enabled in the interface mode (config-if), and if global unicast and anycast IPv6 addresses are not configured, the link-local address is downloaded to the hardware. Otherwise, the lowest IPv6 address is downloaded to hardware.

Conditional Policing Feature of QoS Limitation

The Conditional Policing feature of Quality of Service (QoS) is not supported in Cisco IOS XE Release 2.1.0

Note
Beginning with Cisco IOS XE Release 2.1.1 and later releases, the Conditional Policing feature of Quality of Service (QoS) is supported. This limitation does not apply to these later releases.

IPSec Anti-Replay Window Size Limitation

The maximum IPSec anti-replay window size supported in Cisco IOS XE Release 2.1.0 is 512.
Maximum Number of IPSec Tunnels Limitation

Up to 2k IPSec tunnels are supported in Cisco IOS XE Release 2.1.0.

Note From Cisco IOS XE Release 2.1.1, up to 4K IPSec tunnels are supported. This 2K limitation does not apply to these later releases.

NBAR Protocol Support Limitation

Note Later releases of NBAR in Cisco IOS XE include support for additional protocols. For information about the NBAR protocol support per Cisco IOS XE release, see the following document: http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/clsfy_traffic_nbar_xe.html

Network Based Application Recognition (NBAR) can only match the following protocols in Cisco IOS XE Release 2.1.0:

- CU-SeeMe
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- Post Office Protocol (POP3)
- Telnet
- Secure HTTP
- Real Time Streaming Protocol (RTSP)
- Session Initiation Protocol (SIP)
- Skype (TCP-only)
- HTTP (no options including url and host)
- File Transfer Protocol (FTP)
- H.323

Police Command Limitation

When using a policer for service policies configured on Multilink PPP (MLP) bundles, the percent version of the police command should be used in Cisco IOS XE Release 2.1.0.

Scaling Limits for MLP

The supported scaling limits for Multilink PPP (MLP) in Cisco IOS XE Release 2.1.0 are as follows:

- 16 10 link T1 bundles
- 27 7 link T1 bundles
- 40 5 link T1 bundles
• 500 single link T1 bundles with LFI

---

**Note**

From Cisco IOS XE Release 2.2.3, the MLP scaling limits have been revised. For information about the revised scaling limits for Cisco IOS XE Release 2.2.3 and later releases, see the “Scaling Limits for MLP” section on page 46.

---

**Router Advertisement and Neighbor Solicitation Processing Limitation**

Router advertisements and neighbor solicitation messages are not processed if IPv6 unicast routing is not configured.

**sVTI, DMVPN, and GRE Tunnel Protection Limitation**

The Cisco ASR 1000 Series Routers do not support sVTI, DMVPN, and GRE tunnel protection with NAT traversal.

---

**Note**

From Cisco IOS XE Release 3.4.1S, the limitation on sVTI and GRE tunnel protection has been revised. For information about the revised limitation for Cisco IOS XE Release 3.4.1S and later releases, see the “Limitations and Restrictions in Cisco IOS XE Release 3.4.1S” section on page 39.

---

**Limitation Related to the Handling of Link-Layer Broadcasts**

According to RFC 1812, a packet must be dropped if the L2 address is a broadcast address and the L3 address is not a multicast address or if the broadcast address is not a valid broadcast address. At present, this is not implemented. Note that a valid broadcast address is defined as one of the following:

- 255.255.255.255
- Subnet broadcast address of the incoming interface
- Subnet network address of the incoming interface
New Features in and Important Notes About Cisco IOS XE 3.5S Releases

This chapter provides information about the new features introduced in the Cisco IOS XE 3.5S releases. In addition, important notes about these releases are included in this chapter.

Cisco IOS XE 3S releases inherit all Cisco IOS XE Release 2 features that were released prior to the introduction of the Cisco IOS XE 3S releases with few exceptions. For information about inherited features that were introduced in Cisco IOS XE 2 releases, for a list of new and changed features, and for important notes that apply to Cisco IOS XE Release 2, see the “New and Changed Information” section in Cisco IOS XE Release 2 Release Notes.

This chapter contains the following sections:

- New and Changed Information, page 53
- Important Notes, page 75

New and Changed Information

The following sections list the new hardware and software features that are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.5S:

- New Hardware Features in Cisco IOS XE Release 3.5.2S, page 54
- New Software Features in Cisco IOS XE Release 3.5.2S, page 54
  - Features Supported on the Cisco ASR 903 Series Routers, page 54
  - Features Supported on the Cisco ASR 1000 Series Routers, page 54
- New Hardware Features in Cisco IOS XE Release 3.5.1S, page 54
- New Software Features in Cisco IOS XE Release 3.5.1S, page 54
  - Features Supported on the Cisco ASR 903 Series Routers, page 54
- New Hardware Features in Cisco IOS XE Release 3.5.0S, page 55
- New Software Features in Cisco IOS XE Release 3.5.0S, page 55
  - Features Supported on the Cisco ASR 903 Series Router, page 56
  - Features Supported on the Cisco ASR 1000 Series Routers, page 65
New Hardware Features in Cisco IOS XE Release 3.5.2S

There are no new hardware features introduced in Cisco IOS XE Release 3.5.2S.

New Software Features in Cisco IOS XE Release 3.5.2S

The following are the new software features introduced in Cisco IOS XE Release 3.5.2S.

Features Supported on the Cisco ASR 903 Series Routers

Egress QoS Marking

Platform: Cisco ASR 903
This feature introduces support for QoS marking on egress interfaces. For detailed information, see the following Cisco document:

Features Supported on the Cisco ASR 1000 Series Routers

IPv6 ACL Extensions for Hop by Hop Filtering

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

New Hardware Features in Cisco IOS XE Release 3.5.1S

There are no new hardware features introduced in Cisco IOS XE Release 3.5.1S.

New Software Features in Cisco IOS XE Release 3.5.1S

The following are the new software features introduced in Cisco IOS XE Release 3.5.1S.

Features Supported on the Cisco ASR 903 Series Routers

MPLS OAM Support for Multisegment Pseudowires (PW)

Platform: Cisco ASR 903
For detailed information, see the following Cisco documents:
New Features in and Important Notes About Cisco IOS XE 3.5S Releases

New and Changed Information


MPLS-TP—MS-PW with Static and Dynamic PW Support

Platform: Cisco ASR 903
For detailed information, see the following Cisco documents:

QoS ACLs for ASR900

Platform: Cisco ASR 903
For detailed information, see the following Cisco documents:

REP—Configurable Timers (REP Fast Hellos)

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

REP-no-edge-neighbor-enhancement

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

SSO Support for REP Fast Hello

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

New Hardware Features in Cisco IOS XE Release 3.5.0S

There are no new hardware features introduced in Cisco IOS XE Release 3.5.0S.

New Software Features in Cisco IOS XE Release 3.5.0S

The following are the new software features introduced in Cisco IOS XE Release 3.5.0S.
Features Supported on the Cisco ASR 903 Series Router

1588-2008 Boundary Clock

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

ACL—Access Control List Source and Destination Address Matching

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

ACL—DSCP Matching

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

ACL—ICMP Code

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

ACL—IP Protocol

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:
Any Transport over MPLS (AToM)—ATM Cell Relay over MPLS: Packed Cell Relay

Platform: Cisco ASR 1000 and Cisco ASR 903
For detailed information, see the following Cisco document:

Any Transport over MPLS (AToM)—Ethernet over MPLS (EoMPLS)

Platform: Cisco ASR 903
For detailed information, see the following Cisco documents:

BFD—Static Route Support

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

BGP Support for BFD

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Bidirectional MPLS-TP LSP

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

CFM Extension for 1+1 Hot-Standby Support

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Circuit Emulation over Packet Switched Network

Platform: Cisco ASR 903
New Features in and Important Notes About Cisco IOS XE 3.5S Releases

For detailed information, see the following Cisco document:

**Cisco ASR 903 MIB Support**

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

**Cisco-BGP-MIBv2**

Platform: Cisco ASR 1000 and Cisco ASR 903
For detailed information, see the following Cisco documents:

**Class-Based Policing**

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

**Class-Based Weighted Fair Queuing (CBWFQ)**

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

**CSL (Cisco Secure Licensing Support) on the Cisco ASR 903**

Platform: Cisco ASR 903
For detailed information, see the following Cisco documents:
For a list of supported licenses, see the following document:

**Ethernet Connectivity Fault Management (E-CFM)**

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:
Ethernet Operations, Administration, and Maintenance (OAM)

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

EVC 2.0—Advanced VLAN Translations and Service Mapping Based on 802.1ah (4500)
(Infrastructure)

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Field Programmable Device Upgrade Tool

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Hot Standby Router Protocol (HSRP)

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Inverse Multiplexing over ATM (IMA)

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

IP 16-Way Equal-Cost Multipath

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

IPv4 Unicast Routing Support

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:
IPv6 Routing—IS-IS Support for IPv6

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

IPv6 Routing—OSPF for IPv6 (OSPFv3)

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

IPv6 Routing—Static Routing

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

IPv6 Switching—CEF/dCEF Support

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

IS-IS Support for BFD over IPv4

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

L2VPN—PW Status for Static PWs

Platform: Cisco ASR 903
For detailed information, see the following Cisco documents:

L2VPN Static to Dynamic PW Interconnection and PW Preferred Path for MPLS-TP Tunnels

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:
New and Changed Information

Modular QoS CLI (MQC)

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

MPLS (Multiprotocol Label Switching)

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

MPLS Forwarding Infrastructure Scalability

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

MPLS TP—IP-Less Configuration of MPLS TP Tunnels

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

MPLS-TP OAM—Continuity Check via BFD

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

MPLS-TP OAM—Fault Management

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

MPLS-TP OAM—GACH

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:
New and Changed Information

**MPLS-TP OAM—Ping/Trace**
Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

**MPLS-TP Path Protection**
Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

**MPLS-TP—PW Redundancy for Static PWs**
Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

**MPLS Virtual Private Networks (VPN)**
Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

**Multicast Source Discovery Protocol (MSDP)**
Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

**Multiprotocol BGP (MP-BGP)—MPLS VPN**
Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

**OSPF Support for BFD over IPv4**
Platform: Cisco ASR 903
For detailed information, see the following Cisco document:
PIM Version 2

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Pluggable Optics Support on the Cisco ASR 903

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Punt Policing and Monitoring on the Cisco ASR 903

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

QoS EXP Matching

Platform: Cisco ASR 903
For detailed information, see the following Cisco documents:

QoS Packet Marking

Platform: Cisco ASR 903
For detailed information, see the following Cisco documents:

REP—(Resilient Ethernet Protocol)

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:
SFP-GE-T Support

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Source Specific Multicast (SSM)

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Source Specific Multicast (SSM) Mapping

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

SSO—BFD

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Support for IEEE 1588-2008 Precision Clock Synchronization Protocol

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Synchronous Ethernet Support

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

T1/E1 Support on ASR900

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:
Trunk EFP Support

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Virtual Private LAN Services (VPLS)

Platform: Cisco ASR 1000 and Cisco ASR 903
For detailed information, see the following Cisco documents:

VPLS MAC Address Withdrawal

Platform: Cisco ASR 1000 and Cisco ASR 903
For detailed information, see the following Cisco document:

VPLS over MPLS-TP

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Y.1731 Performance Monitoring

Platform: Cisco ASR 903
For detailed information, see the following Cisco document:

Features Supported on the Cisco ASR 1000 Series Routers

1 Second Accuracy—IPv6 Session Counters and ISGv6 Services

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

Alarm-Related Enhancements

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

**ALG—SCCP v17 Support**

Platform: Cisco ASR 1000
For detailed information, see the following Cisco documents:

**Any Transport over MPLS (AToM)—ATM Cell Relay over MPLS: Packed Cell Relay**

Platform: Cisco ASR 1000 and Cisco ASR 903
For detailed information, see the following Cisco document:

**ASR1K FRF.12 Support on MFR Interfaces**

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

**ATM Port Mode Packed Cell Relay over MPLS**

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

**BFD on BDI Interfaces**

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

**BGP—Origin AS Validation**

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:
CAC-Related Enhancements

Platform: Cisco ASR 1000

For detailed information, see the following Cisco document:

Category and Attribute Optional Template Export via FNF

Platform: Cisco ASR 1000

For detailed information, see the following Cisco document:

Cisco-BGP-MIBv2

Platform: Cisco ASR 1000 and Cisco ASR 903

For detailed information, see the following Cisco document:

DHCPv6—Relay Chaining (for Prefix Delegation) and Route Insertion in FIB

Platform: Cisco ASR 1000

For detailed information, see the following Cisco document:

DT QoS Accounting HA

Platform: Cisco ASR 1000

For detailed information, see the following Cisco document:

E3 Support for SPA-2CHT3-CE-ATM on ASR1K

Platform: Cisco ASR 1000

For detailed information, see the following Cisco document:

Embedded Event Manager (EEM) 4.0

Platform: Cisco ASR 1000

For detailed information, see the following Cisco document:

Enhancement of Out of Order Packet Handing in ZBFW

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

ERSPAN Support on WAN Interface

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

Extensible Messaging Client Protocol (XMCP) 2.0

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

Flexible NetFlow—Ingress VRF Support

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

FTP64 NAT ALG Intrabox HA Support

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:
IGMP Snooping
Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

IKEv2 Headend Support for Remote Access Clients—Anyconnect, Win7 IPv6, Flexvpn Hardware
Client. Multi SA Support for VTI
Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

Inter-Chassis Asymmetric Routing Support for Zone-Based Firewall and NAT
Platform: Cisco ASR 1000
For detailed information, see the following Cisco documents:
l
l

IPv6 Client Support on Proxy Mobile IPv6 Mobile Access Gateway
Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

IPv6 over v4 GRE Tunnel Protection
Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

ISG Policy HA and Rabapol HA
Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:
ISG—Flow Control: SSO/ISSU

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

ISG—IPv6 Support Phase II

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

L2TP Attributes Physical Channel ID and Initial Received LCP

Platform: Cisco ASR 1000
The L2TP Attributes Physical Channel ID and Initial Received feature introduces two new keywords—Physical Channel ID and Initial Received—to the vpdn l2tp attribute command. These keywords enable the sending of attribute-value pairs in session creation packets from the L2TP (Layer 2 Tunneling Protocol) Access Concentrator (LAC) to the L2TP Network Server (LNS). For more information, please refer to the vpdn l2tp attribute command page.

Layer 4 Redirect Logging Enhancement

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

Line-Side Support for Cisco Unified Communications Manager

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

LISP Virtualization

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

LNS Cluster/Dead Cache Optimization

Platform: Cisco ASR 1000
The LNS Cluster/dead cache optimization feature introduces two new states—TESTABLE and TESTING—in the output of the `show vpdn dead-cache` command. These states indicate when the L2TP (Layer 2 Tunneling Protocol) Network Server (LNS) starts and exits the testing state. For more information, please refer to the `show vpdn dead-cache` command page.

**MediaTrace 1.0**

Platform: Cisco ASR 1000

For detailed information, see the following Cisco document:


**MPLS Diff-Serv-Aware Traffic Engineering (DS-TE)**

Platform: Cisco ASR 1000

For detailed information, see the following Cisco document:


**MPLS TE—Autoroute Destinations**

Platform: Cisco ASR 1000

For detailed information, see the following Cisco document:


**MPLS TE—Autotunnel/Automesh SSO Coexistence**

Platform: Cisco ASR 1000

For detailed information, see the following Cisco documents:


**MPLS TE—DS-TE (RFC-3270)**

Platform: Cisco ASR 1000

For detailed information, see the following Cisco document:


**MPLS TE—Enhanced Path Protection**

Platform: Cisco ASR 1000

For detailed information, see the following Cisco document:
MPLS TE—RSVP Graceful Restart 12.0S-12.2S Interop

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

MPLS Traffic Engineering (TE)—Interarea Tunnels

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

MPLS Traffic Engineering—Inter-AS TE

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

MPLS Traffic Engineering—Shared Risk Link Groups (SRLG)

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

MsRPC AIC Support for FW and NAT

Platform: Cisco ASR 1000
For detailed information, see the following Cisco documents:

NBAR Classification Enhancements for IOS XE 3.5

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:
Nested Class-Map Support for ZBFW

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

NTPv4 Orphan Mode Support, Range for Trusted Key

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

OTV—Overlay Transport Virtualization

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

Performance Monitor (Phase 1)

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

Performance Monitor (Phase 2)

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

Pfr SNMP MIB v1.0 (Read-Only)

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

Pfr Target Discovery v1.0

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:
PPP—IPv4 Address Conservation in Dual Stack Environments

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

PPP over Ethernet Client

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

QoS—Tunnel Marking for GRE Tunnels

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

RaBaPol Web Traffic L4 Redirect Logging Enhancement

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

RADIUS-BASED Lawful Intercept High Availability

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

Stateful NAT64—Intra-Chassis Redundancy

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:

Support match-in-vrf Keyword for ASR1k NAT

Platform: Cisco ASR 1000
For detailed information, see the following Cisco document:
**Trustsec SG Firewall Enforcement IPv4**

Platform: Cisco ASR 1000

For detailed information, see the following Cisco documents:


**Virtual Private LAN Services (VPLS)**

Platform: Cisco ASR 1000 and Cisco ASR 903

For detailed information, see the following Cisco documents:


**VPLS MAC Address Withdrawal**

Platform: Cisco ASR 1000 and Cisco ASR 903

For detailed information, see the following Cisco document:


**Important Notes**

The following sections contain important notes about Cisco IOS XE 3S Releases running on Cisco ASR 1000 Series Routers.

**Deferrals**

Cisco IOS software images are subject to deferral. We recommend that you view the deferral notices at the following location to determine whether your software release is affected:


**Field Notices and Bulletins**

- Field Notices—We recommend that you view the field notices for this release to determine whether your software or hardware platforms are affected. You can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Important Notes About IPSec Support on the Cisco ASR 1000 Series Router

This section contains important notes about IPSec support on the Cisco ASR 1000 Series Router:

**IPSec CLI Support Notes**

This section contains important notes about IPSec CLI support on the Cisco ASR 1000 Series Router.

For information about Cisco IOS IPSec commands, see *Cisco IOS Security Command Reference* at the following location:


- The *show crypto engine* command, which displays information about the crypto engine, is not currently supported on the Cisco ASR 1000 Series Router. The unsupported *show crypto engine* subcommands include the following:
  - *accelerator* (Shows crypto accelerator information.)
  - *brief* (Shows all crypto engines in the system.)
  - *configuration* (Shows crypto engine configuration.)
  - *connections* (Shows connection information.)
  - *qos* (Shows QoS information.)

- The Cisco ASR 1000 Series Router does not currently support the display of send and recv error statistics using the *show crypto ipsec sa identity* command.

- The Cisco ASR 1000 Series Router does not support the *clear* and *show crypto* commands on the standby Route Processor (RP) by design.

- Counters in the *show platform software ipsec fp active flow identifier n* command are flagged for reset on read. You can use the *show crypto ipsec sa* command to obtain integral counters.

- The *show access-list* command output does not show a packet count matching the ACL.

- The Cisco ASR 1000 Series Router displays debugging information about the consumption of IPsec datapath memory; use the *show platform hardware qfp act feature ipsec datapath memory* command in privileged EXEC or diagnostic mode.

- The Cisco ASR 1000 Series Router displays debugging information about the crypto engine processor registers; use the *show platform software ipsec f0 encryption-processor registers* command in privileged EXEC or diagnostic mode.

**Crypto Map Support**

This section contains important notes about IPSec crypto map support on the Cisco ASR 1000 Series Router:

- The Cisco ASR 1000 Series Router does not currently support IPSec tunnel configuration for crypto maps with same IP address on both the tunnel interface and the physical interface. Configurations with different IP addresses are supported.

- A possible Embedded Services Processor (ESP) reload may occur if a large number (such as 2000) of crypto maps are removed simultaneously. When removing a large number of crypto maps, it is recommended you unconfigure 500 crypto maps at a time and wait 25 seconds between operations.

- The Cisco ASR 1000 Series Router does not support the *show access-lists id* command under crypto maps.

- The Cisco ASR 1000 Series Router does not currently support the *interface range* command when configuring crypto maps.
**IPSec Packet Processing**

This section contains important notes about IPSec packet processing on the Cisco ASR 1000 Series Router:

- Reloading an Embedded Services Processor (ESP) on the Cisco ASR 1000 Series Router may cause a few IPSec packets to drop before the initialization completes, but the traffic will resume after a brief interval.
- The Cisco ASR 1000 Series Router will not discard an incoming IP datagram containing a Payload Length other than 4 in the authentication header (AH). For example, a 96 bit authentication value plus the 3 32-bit word fixed portion for any non-null authentication algorithm will not be discarded.
- The Cisco ASR 1000 Series Router does not forward incoming authenticated packets with the IP option field set.

**GET VPN Support**

This section contains important notes about Group Encrypted Transport VPN (GET VPN) support on the Cisco ASR 1000 Series Router:

- To ensure normal traffic flow for a GET VPN configuration on a Cisco ASR 1000 Series Router, a Time Based Anti Replay (TBAR) window-size of greater than 42 seconds is recommended.
- The Cisco ASR 1000 Series Router does not currently support the TBAR statistics display in the `show crypto gdoi gm replay` command.
- The Cisco ASR 1000 Series Router does not currently support Easy VPN (EzVPN) and GET VPN on the same interface.
- When a Cisco ASR 1000 Series Router is to apply the same Group Domain of Interpretation (GDOI) crypto maps to two interfaces, you should use local addresses for the crypto maps. Non-local address configuration is not supported.
- The Cisco ASR 1000 Series Router does not currently support transport mode for TBAR.
- The Cisco ASR 1000 Series Router only supports the reassembly of post-fragmented GET VPN packets that are destined for the local Cisco ASR 1000 Series Router in the GET VPN network.
- An enhancement is added to enable reassembly of IPSec transit traffic. This enhancement applies only to post-encryption fragmented IPSec packets. When this enhancement is enabled, IPSec will detect transit IPSec traffic and reassemble it before decryption. GET VPN transit IPSec traffic will be reassembled, decrypted, and forwarded to the destination. Non GET VPN transit IPSec traffic will be reassembled but not decrypted (because the Cisco ASR 1000 router is not the IPSec tunnel end point) and then forwarded to the destination.

To enable IPSec reassembly of transit traffic, use the `platform ipsec reassembly transit` command in global configuration mode. To disable IPSec reassembly of transit traffic, use the `no` form of this command.

```
platform ipsec reassembly transit
[no] platform ipsec reassembly transit
```

**IPSec SSO and ISSU Support Notes**

- The Cisco ASR 1000 Series Router supports stateful IPSec sessions on ESP switchover. During ESP switchover, all IPSec sessions will stay up and no user intervention is needed to maintain IPSec sessions.
• For an ESP reload (no standby ESP), the SA sequence number restarts from 0. The peer router drops packets that do not have the expected sequence number. User may need to explicitly reestablish IPSec sessions to work around this issue for systems that have a single ESP after an ESP reload. User may experience traffic disruption over the IPSec sessions in such cases for the duration of the reload.

• The Cisco ASR 1000 Series Router currently does not support Stateful Switchover (SSO) IPSec sessions on Route Processors (RPs). The IPSec sessions will go down on initiation of the switchover, but will come back up when the new RP becomes active. No user intervention is needed. User will experience traffic disruption over the IPSec sessions for the duration of the switchover, until the sessions are back up.

• The Cisco ASR 1000 Series Router currently does not support stateful ISSU for IPSec sessions. Before performing an ISSU, users must explicitly terminate all existing IPSec sessions or tunnels prior to the operation and reestablish them post ISSU. Specifically, users must ensure that there are no half-open or established IPSec tunnels present before performing ISSU. To do this, we recommend user do a interface shutdown in the case of interfaces that may initiate a tunnel setup, such as a routing protocol initiating a tunnel setup, or interfaces that have keepalive enabled or where there is an auto trigger for an IPSec session. Traffic disruption over the IPSec sessions during ISSU is obvious in this case.

Summarizing Caveats
• ESP—Switchover (with standby ESP): Stateful: IPSec sessions should be up. No user intervention needed.
• ESP—Reload (no standby ESP): Stateless: IPSec sessions will go down and come back. Usually, no user intervention is needed. However, users may have to explicitly re-establish an IPSec session if antireplay is configured (sequence number checking).
• RP—Switchover (with standby RP): Stateless: IPSec sessions will go down on RP switchover and the session should re-establish automatically when the new RP gains an active role. No user intervention is needed.
• ISSU (irrespective of chassis type): Stateless: Users must explicitly terminate all the IPSec sessions by shutting the interfaces, perform ISSU, and then re-establish tunnels by enabling the interfaces. No other intervention is needed.

Miscellaneous IPSec Support Notes
This section contains miscellaneous important notes about IPSec support on the Cisco ASR 1000 Series Router:
• In the context of an IPSec DVTI connection, the Cisco ASR 1000 Router does not support dynamic download ACL rule (per-user attribute) from the AAA server.

For example, the following configurations are not supported:

```
cisco-avpair += "ip:inacl#1=permit ip any 2.2.2.0 0.0.0.255"
cisco-avpair += "ip:outacl#1=permit ip 2.2.2.0 0.0.0.255 any"
```

• The Cisco ASR 1000 Router does not support the command of “if-state nhrp” in configuring the tunnel.
• The Cisco ASR 1000 Router Dead Peer Detection behavior is different than the pre-defined behavior (i.e. when there is no traffic to be sent, no DPD is sent, while if any traffic to be sent, DPD is sent). A Cisco ASR 1000 Router DPD is sent out regardless there is outbound traffic needs to be sent out.
• The Cisco ASR 1000 Router does not support SA Path MTU on data path.
• The Cisco ASR 1000 Router does not support double ACL in dynamic crypto map.
Important Notes

- VRF without crypto map configured on a physical interface causes dual esp reload on a Cisco ASR 1000 Router.
- The command: `show crypto ipsec sa identity` does not log send and receive error counts.
- The commands: `clear crypto` and `show crypto` on Standby RP are inconsistent with Active RP. At present most of other features disable ‘clear commands’ from Standby RP, but IPSec still allows to clear sa, session etc. from the standby.
- The Cisco ASR 1000 Router does not support Cisco AAA av-pair “cisco-avpair += ip:sub-policy-In=policy1”.
- CLI allows both ikev1 and ikev2 profile configured under the same crypto map, even though it is not supported internally on the ASR 1000 Router.
- For a Cisco ASR 1000 Router, the tunnel protection should be removed first before changing any configuration for tunnel protection.
- The security association (SA) maximum transmission unit (MTU) calculation is based on the interface MTU instead of the IP MTU.
- The Cisco ASR 1000 Series Router currently supports a maximum anti-replay window value of 512. If you attempt to configure a value larger than 512, the Cisco ASR 1000 Series Router defaults back to 512 internally (although the display still shows your user-configured value).
- The Cisco ASR 1000 Series Router does not currently support nested SA transformation such as:
  ```plaintext
  crypto ipsec transform-set transform-1 ah-sha-hmac esp-3des esp-md5-hmac
  crypto ipsec transform-set transform-1 ah-md5-hmac esp-3des esp-md5-hmac
  ```
- The Cisco ASR 1000 Series Router does not currently support Cisco IOS Certificate Authority (CA) server features.
- The Cisco ASR 1000 Series Router does not currently support COMP-LZS configuration.
- On Cisco ASR 1000 Series Routers, when configuring GRE over IPSec, it is recommended that you use only the tunnel protection mode on the tunnel interface. Using crypto maps on both the tunnel interface and the physical interface to achieve GRE over IPSec is not the supported method of configuration.
- When using dynamic VTI-based IPSec on a Cisco ASR 1000 Router, if there are multiple remote IPSec endpoints behind the same NAT device, only one of the endpoints has connectivity. In other words, multiple endpoints cannot have connectivity at the same time.

NAT and Firewall ALG Support on the Cisco ASR 1000 Series Routers

*NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers* matrix summarizes Network Address Translation (NAT) and Firewall Application Layer Gateway (ALG) feature support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1.0 and later releases. The matrix lists feature support by release. NAT and Firewall ALG support is cumulative; features introduced in earlier releases continue to be supported in later releases. You can find the matrix at the following location:


Important Notes About Cisco IOS XE Release 3.5.0S

This section describes important notes about Cisco IOS XE Release 3.5.0S and later releases.
**Cisco ASR 903 Images**

Cisco engineering has removed the following images from Cisco.com:

- `asr903rsp1-universalk9_npe.03.05.00.S.152.S.bin`
- `asr903rsp1-universal.03.05.00.S.152-1.S.bin`

Please use the following new images from Cisco.com:

- `asr903rsp1-universalk9_npe.03.05.00.S.152.S0a.bin`
- `asr903rsp1-universal.03.05.00.S.152-1.S0a.bin`

**Propagating Traffic Priorities to Higher Levels**

Priority propagation ensures that the appropriate priority is maintained for particular traffic classes throughout all levels of the queueing and scheduling hierarchy. When propagating oversubscribed priority traffic to higher levels in the hierarchy, the rate ratios for these traffic classes are relative to the shaping rates for the immediate parent classes of the priority queues(s). This is demonstrated in the example below.

```
> policy-map Parent
>  class class-default
>  shape average 100000000
>  service-policy Child
>  policy-map Child
>    class class1
>    shape average 50000000
>    service-policy Grand-child1
>    class class2
>    shape average 40000000
>    service-policy Grand-child2
>    class class3
>    shape average 30000000
>    service-policy Grand-child3
>  policy-map Grand-child1
>    class classA
>    priority
>  policy-map Grand-child2
>    class classB
>    priority
>  policy-map Grand-child3
>    class classC
>    priority
```

In the above example, the “Parent” policy-map is oversubscribed, but when traffic is congested, the rates for the priority traffic in class1, class2, and class3 are only allowed as shown below due to priority propagation.

- class1: 41.7Mbps (=100Mbps/120Mbps * 50Mbps)
- class2: 33.3Mbps (=100Mbps/120Mbps * 40Mbps)
- class3: 25.0Mbps (=100Mbps/120Mbps * 30Mbps)

**Important Notes About Cisco IOS XE Release 3.4.1S**

This section provides important notes about Cisco IOS XE Release 3.4.1S.
BGP Scan Time Range

The `bgp scan-time` command has a scanner-interval range of 5-60 seconds. The `bgp scan-time` command can be configured, even if BGP Next Hop Tracking (NHT) is configured (by the `bgp nexthop` command).

Important Notes About Cisco IOS XE Release 3.3.1S

This section provides important notes about Cisco IOS XE Release 3.3.1S.

Broadband Encapsulation Autosense Support Notes

This section contains important notes about the support for broadband encapsulation autosense with RBE configuration in Cisco IOS XE Release 3.3.1S:

- The broadband encapsulation autosense enhancement enables broadband autosense support for PPPoEoA, PPoA, and RBE.
- In the Cisco IOS XE releases prior to Release 3.3.1S, aal5autopp encapsulation was not supported when an RBE was configured. As a result, the combination of aal5autopp encapsulation with RBE was not supported in the Cisco IOS XE releases prior to Release 3.3.1S.

The broadband encapsulation enhancement in Cisco IOS XE Release 3.3.1S supports the combination of aal5autopp encapsulation with RBE-related configurations.

Important Notes About Cisco IOS XE Release 3.3.0S

This section provides important notes about Cisco IOS XE Release 3.3.0S and later releases.

High Availability on SBC

The following is the expected behavior of a session border controller (SBC) on which the High Availability feature is configured:

If switchover occurs while an H.323–H.323 T.38 fax transmission is in progress, the call does not fall back to the voice mode after the completion of the fax transmission. This is because the signaling state is not preserved in the event of a switchover.

IPsec Failover

IPSec failover is a feature that increases the total uptime (or availability) of your IPSec network. Traditionally, this is accomplished by employing a redundant (standby) router in addition to the original (active) router. If the active router becomes unavailable for any reason, the standby router takes over the processing of IKE and IPSec.

IPSec failover falls into two categories: stateless failover and stateful failover. The IPSec on the Cisco ASR 1000 Series Router supports only stateless failover. Stateless failover uses protocols such as the Hot Standby Router Protocol (HSRP) to provide primary to secondary cutover and also allows the active and standby VPN gateways to share a common virtual IP address.
Important Notes About Cisco IOS XE Release 3.2.1S

This section describes important notes about Cisco IOS XE Release 3.2.1S and later releases.

EzVPN Support on Cisco ASR 1000 Series Routers

On a ASR Cisco 1000 Router, when an EzVPN session is ended, the EzVPN server sends out a Stop Accounting message. This message does not contain the Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, and Acct-Output-Packets fields. It might cause a disruption of accounting performed on traffic.

Maximum IP MTU for Loopback Interfaces

For loopback interfaces, the maximum IP MTU is now 4000. This is to match the serial interface limits.

Important Notes About Cisco IOS XE Release 3.2.0S

This section describes important notes about Cisco IOS XE Release 3.2.0S and later releases.

Cisco ASR 1001-4XT3

Cisco ASR1001-4XT3 chassis functionality is similar to the SPA-4XT3/E3 with the exception of E3 circuitry in Cisco IOS XE 3.2.0S Release.

SIP Trunk Over TCP

SIP TCP trunk calls may not activate if more than one complete SIP messages were contained in one TCP segment in Cisco IOS XE 3.2.0S Release.

This symptom occurs upon SIP trunk over TCP scenario. SIP ALG currently processes only one complete SIP message in one TCP segment (one complete or one complete plus one incomplete), refer to CSCti56370.

TCP Failover in Hardware High-Availability Mode

TCP failover is not supported in Hardware High-Availability mode. If the active node fails in Hardware High Availability mode and if the network is restored, it may take 5 to 10 minutes for the standby node to become the active node. This is because of the reboot and the peer negotiation delay. If the network is not restored, only the switched over active peer is available. Failover is not possible in this state.

Extended ACL as a WCCP Redirect ACL

The Cisco ASR 1000 Series Router supports the use of an extended ACL as a WCCP redirect ACL. However, the option to specify a port range is not supported.
Important Notes About Cisco IOS XE Release 3.1.1S

This section describes important notes about Cisco IOS XE Release 3.1.1S and later releases.

SIP-40G:SPA-4XT-Serial

Cisco SPA-4XT-Serial was not supported in 3.1.0S when plugged into an ASR1000 with SIP-40. This SPA is supported in Release 3.1.1S on SIP-40 linecard.

For more information, see the following documents:
Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation, see section for SPA-4XT-Serial SPA in Table 1-4 (SIP and SPA Compatibility for Serial SPAs).
Cisco ASR1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide

Important Notes About Cisco IOS XE Release 3.1.0S

This section describes important notes about Cisco IOS XE Release 3.1.0S and later releases.

Bidirectional Forwarding Detection (BFD)

In Cisco IOS XE Release 3.1.0S, Bidirectional Forwarding Detection (BFD) is no longer supported in IP Base software packages. For BFD support, use the Advanced IP Services or Advanced Enterprise Services packages.

DMVPN Spoke Support

In Cisco IOS XE Release 3.1.0S Cisco ASR 1000 Series Routers do not support the ip nhrp server-only command if they act as DMVPN spokes.

Important Notes About Cisco IOS XE Release 2.6.0

This section describes important notes about Cisco IOS XE Release 2.6.0 and later releases.

Per-User Attribute on PPP Virtual Access

In Cisco IOS XE Release 2.6.0 multiple instances of the per-user attribute ‘Cisco-Avpair=lcp:interface-config=<cmd>’ is not supported.

For example:
Cisco-AVPair = lcp:interface-config=ip vrf forwarding vpngreen
Cisco-AVPair= lcp:interface-config=ip unnumbered loopback2
New Features in and Important Notes About Cisco IOS XE 3.5R Releases

Important Notes

Should be configured like this in Cisco IOS XE Release 2.6.0:
Cisco-AVPair = lcp:interface-config=ip vrf forwarding vpn green \nip unnumbered loopback2
“Multiple instances will be supported in Cisco IOS XE Release 2.6.1”

Legacy QoS Command Deprecation: Hidden Commands

To streamline Cisco IOS QoS (quality of service), certain commands are being hidden. Although these commands are available in Cisco IOS XE Release 2.6, the CLI interactive help does not display them. If you attempt to view a command by entering a question mark at the command line, the command does not appear. However, if you know the command syntax, you can enter it. The system will accept the command and return a message explaining that it will soon be removed. These commands will be completely removed in a future release, which means that you will need to use the appropriate replacement commands.

For more information, see the following document:

VRF-Aware NAT

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.5.0

This section describes important notes about Cisco IOS XE Release 2.5.0 and later releases.

Embedded Packet Capture

The Embedded Packet Capture (EPC) feature is not functional and not supported for the Cisco ASR 1000 Series Routers.

QoS: Policing Support for GRE Tunnels

When queuing feature on the GRE tunnel interface is not supported with crypto configured on the physical interface.

QoS: Support for GRE/sVTI Tunnel

With IOS XE 2.5.0, the Cisco ASR 1000 Router Series supports Quality-of-Service (QoS) applied to:

- A GRE or sVTI tunnel with policing and marking only for INGRESS traffic
- A GRE or sVTI tunnel with 2-level hierarchy allowing queuing on the second level for EGRESS traffic

When there are multiple egress physical interfaces for a tunnel, and the tunnel target physical interface changes as a result of tunnel target destination route change, either manually by user configuration or by routing protocol, IOS will not prevent the tunnel traffic from moving to an alternate egress physical
interface. However, in IOS XE 2.5.0, QoS tunnel move feature is not supported. When tunnel traffic moved to an alternate egress physical interface, tunnel QoS policy may enter a suspended state. At this point, the tunnel QoS policy will have to be removed and reapplied to the tunnel interface for it to take effect. In addition, queuing features on the GRE tunnel interface are not supported when IPSec is configured on the physical interface.

VRF-Aware NAT

Integrating NAT with MPLS VPNs

This section provides information about integrating NAT with MPLS VPNs.

Prerequisites for Integrating NAT with MPLS VPNs

Before performing the tasks in this module, you should be familiar with the concepts related to configuring NAT for IP address conservation. All access lists required for use with the tasks in this module should be configured prior to beginning the configuration task. For information about how to configure an access list, see IP Access List Sequence Numbering at the following location:


Note: If you specify an access list to use with a NAT command, NAT does not support the commonly used permit ip any command in the access list.

Restrictions for Integrating NAT with MPLS VPNs

- The following functionality is not supported for VRF-Aware NAT:
  - VPN to VPN translations. In other words, VRF cannot be applied on the NAT outside interface.
  - Translation of multicast packets
  - Translations with inside destinations
  - Reversible route maps
  - MIBs
  - MPLS traffic engineering
- Configuring inside dynamic translations defined with outside interface mappings is not supported.
- Configuring inside static translations with interface mappings is not supported. The following commands, which do not include VRF, are not supported:
  - ip nat inside source static esp local-ip interface type number
  - ip nat inside source static local-ip global-ip route-map name
  - ip nat inside source static local-ip interface type number
  - ip nat inside source static tcp local-ip local-port interface type number global-port
  - ip nat inside source static udp local-ip local-port interface type number global-port

Dependency of NAT on VFR

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.
Important Notes About Cisco IOS XE Release 2.3.0

This section describes important notes about Cisco IOS XE Release 2.3.0 and later releases.

Any Transport Over MPLS (AToM) Support

The configuration of Any Transport Over MPLS (AToM) on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.3.0 is only supported on a subinterface; AToM cannot be configured on the main interface. In addition, you cannot have any IP configuration on the main interface when you have an AToM configuration on the subinterface. These configuration guidelines are applicable to VC mode, VP mode, and L2VPN PW redundancy.

MPLS TE Support

Cisco ASR 1000 Series Router users considering the implementation of MPLS TE are recommended to consult with their local Cisco technical support representative for Cisco IOS XE implementation details.

VRF-Aware NAT

Dependency of NAT on VFR

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.2.2

This section describes important notes about Cisco IOS XE Release 2.2.2 and later releases.

SSO for L2TP Tunnel Switching Not Supported

If dual route processors (RPs) are used on the Cisco ASR 1000 Series Router in Cisco IOS XE Release 2.2.2 and L2TP Tunnel Switching is configured, then no l2tp sso enable must be configured.

VRF-Aware NAT

Dependency of NAT on VFR

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces and environments in Cisco IOS XE Release 2.2.2. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.2.1

This section describes important notes about Cisco IOS XE Release 2.2.1 and later releases.
100M FX SFP Not Supported on Cisco 2-Port Gigabit Ethernet Shared Port Adapter

The 100M FX SFP is not supported on the Cisco 2-Port Gigabit Ethernet Shared Port Adapter (2x1GE SPA) on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2.1.

Intelligent Service Gateway (ISG) Features Not Supported

The following Intelligent Service Gateway (ISG) features are not supported on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2.1:

- ISG IP subscriber functionality on the following types of access interfaces: Gigabit EtherChannel (GEC) (Port Channel), generic routing encapsulation (GRE), PPP (virtual-template), and Layer 2 Tunneling Protocol (L2TP)
- ISG prepaid billing
- ISG IP interface sessions
- Interface statistics for ISG multiservice interfaces
- Access lists cannot be configured as match criteria in ISG Layer 4 redirect configuration. As an alternative, Layer 4 redirect should be configured in ISG traffic class services.
- Stateful Switchover (SSO and in-service software upgrade (ISSU) for ISG IP subscriber sessions or traffic class sessions. Upon switchover, an IP session must be recreated or restarted (for Dynamic Host Configuration Protocol (DHCP) sessions) when the session becomes active again.
- SSO and ISSU for any features on IP subscriber sessions or traffic class class sessions
- SSO and ISSU for the following features on ISG PPP sessions:
  - Port-Bundle Host Key
  - Layer 4 Redirect
  - Traffic Class

Per-Session Multicast Support

Enhancements to the IP multicast feature provide support for per-session multicast in broadband environments in Cisco IOS XE Release 2.2.1.

VRF-Aware NAT

Dependency of NAT on VFR
ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces and environments in Cisco IOS XE Release 2.2.1. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.1.1

This section describes important notes about Cisco IOS XE Release 2.1.1 and later releases.
Important Notes

Startup Configuration File Backup

As a matter of routine maintenance on any Cisco router, users should backup the startup configuration file by copying the startup configuration file from NVRAM onto one of the router’s other file systems and, additionally, onto a network server. Backing up the startup configuration file provides an easy method of recovering the startup configuration file in the event the startup configuration file in NVRAM becomes unusable for any reason.

For users using any Cisco ASR 1000 Series Router with a single RP, including any Cisco ASR 1002 or Cisco ASR 1004 Router, backing up the startup configuration file onto another router file system is especially important due to CSCsq70140, which is documented in the Caveats section of these release notes. The workaround for users who run into this caveat is to replace the startup configuration file in NVRAM with a backup copy of the startup configuration file on the router; therefore, customers who have backed up their startup configuration files onto the router will be ready to resolve these caveats if they occur on their Cisco ASR 1000 Series Routers using a single RP.

Example 1: Copying Startup Configuration File to Bootflash

Router# dir bootflash:
Directory of bootflash:/

```
  11 drwx  16384 Dec 4 2007 04:32:46 -08:00 lost+found
 86401 drwx  4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx  4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx  4096 May 29 2008 16:31:41 -07:00 .prst_sync
43201 drwx  4096 Dec 4 2007 04:34:45 -08:00 .installer
 12 -rw- 208904396 May 28 2008 16:17:34 -07:00 asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin
```

Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]?

```
3517 bytes copied in 0.647 secs (5436 bytes/sec)
```

Router# dir bootflash:
Directory of bootflash:/

```
  11 drwx  16384 Dec 4 2007 04:32:46 -08:00 lost+found
 86401 drwx  4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx  4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx  4096 May 29 2008 16:31:41 -07:00 .prst_sync
43201 drwx  4096 Dec 4 2007 04:34:45 -08:00 .installer
 12 -rw- 208904396 May 28 2008 16:17:34 -07:00 asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin
13 -rw-  7516 Jul 2 2008 15:01:39 -07:00 startup-config
```

Example 2: Copying Startup Configuration File to USB Flash Disk

Router# dir usb0:
Directory of usb0:/

```
 43261 -rw- 208904396 May 27 2008 14:10:20 -07:00 asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin
```

```
255497216 bytes total (40190464 bytes free)
```

Router# copy nvram:startup-config usb0:
Destination filename [startup-config]?

```
3172 bytes copied in 0.214 secs (14822 bytes/sec)
```

Router# dir usb0:
Important Notes

Directory of usb0:/

43261 -rwx 208904396 May 27 2008 14:10:20 -07:00
asr1000rpl-adventerprisek9.02.01.00.122-33.XNA.bin
43262 -rwx 3172 Jul 2 2008 15:40:45 -07:00 startup-config

255497216 bytes total (40186880 bytes free)

Example 3: Copying Startup Configuration File to a TFTP Server

Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.17.16.81
Destination filename [pe24_asr-1002-config]? /auto/tftp-users/user/startup-config
!!
3517 bytes copied in 0.122 secs (28828 bytes/sec)

VRF-Aware NAT

Dependency of NAT on VFR

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.1.0

This section describes important notes about Cisco IOS XE Release 2.1.0 and later releases.

High-Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers

Table 1 describes some of the high level feature sets that are not supported for the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1.0 and later releases. Use Cisco Feature Navigator to confirm support for a specific feature. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note

Feature support is subject to change from release to release. Some high-level feature sets that were not supported in the initial Cisco IOS XE Release 2.1.0 are now supported. Table 1 has been updated to indicate when support has been introduced in later releases. For the latest feature information, see the New and Changed Information sections of these release notes and Cisco Feature Navigator.

<table>
<thead>
<tr>
<th>Major Feature Category</th>
<th>Features Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>Support for ATM features begins in Cisco IOS XE Release 2.3.0. No ATM features are supported in earlier releases.</td>
</tr>
<tr>
<td>Broadband</td>
<td>Support for ANCP begins in Cisco IOS XE Release 2.4.0. ANCP is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>IPv6 Intelligent Service Gateway (IPv6 ISG)</td>
</tr>
<tr>
<td></td>
<td>Point-to-Point Protocol over Ethernet Tag (PPPoE Tag)</td>
</tr>
<tr>
<td></td>
<td>PPP over Q-in-Q (PPPoQinQ)</td>
</tr>
</tbody>
</table>
## Important Notes

### Ethernet OAM
- Ethernet Operation, Administration, and Maintenance (OAM)

### MPLS
- Support for Carrier’s Carrier begins in Cisco IOS XE Release 2.2.3. Carrier’s Carrier is not supported in earlier releases.
- Support for Ethernet over MPLS (EoMPLS) begins in Cisco IOS XE Release 2.4.0. Ethernet over MPLS (EoMPLS) is not supported in earlier releases.
- Support for Inter-AS begins in Cisco IOS XE Release 2.2.2. Inter-AS is not supported in earlier releases.

### IPv6 Provider Edge Router over MPLS (6PE)

### IPv6 VPN over MPLS (6VPE)

### Label Distribution Protocol (LDP) Session Protection

### Support for Layer 2 VPN (L2VPN) begins in Cisco IOS XE Release 2.3.0. L2VPN is not supported in earlier releases.

### Support for MPLS Traffic Engineering/Fast Reroute (MPLS TE/FRR) begins in Cisco IOS XE Release 2.3.0. MPLS TE/FRR is not supported in earlier releases.

### Virtual Private LAN Service (VPLS)

## Table 1
**High-Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers (continued)**

<table>
<thead>
<tr>
<th>Major Feature Category</th>
<th>Features Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ethernet OAM</strong></td>
<td>Ethernet Operation, Administration, and Maintenance (OAM)</td>
</tr>
<tr>
<td><strong>MPLS</strong></td>
<td>Support for Carrier’s Carrier begins in Cisco IOS XE Release 2.2.3. Carrier’s Carrier is not supported in earlier releases. Support for Ethernet over MPLS (EoMPLS) begins in Cisco IOS XE Release 2.4.0. Ethernet over MPLS (EoMPLS) is not supported in earlier releases. Support for Inter-AS begins in Cisco IOS XE Release 2.2.2. Inter-AS is not supported in earlier releases. IPv6 Provider Edge Router over MPLS (6PE) IPv6 VPN over MPLS (6VPE) Label Distribution Protocol (LDP) Session Protection Support for Layer 2 VPN (L2VPN) begins in Cisco IOS XE Release 2.3.0. L2VPN is not supported in earlier releases. Support for MPLS Traffic Engineering/Fast Reroute (MPLS TE/FRR) begins in Cisco IOS XE Release 2.3.0. MPLS TE/FRR is not supported in earlier releases. Virtual Private LAN Service (VPLS)</td>
</tr>
</tbody>
</table>
New Features in and Important Notes About Cisco IOS XE 3.4S Releases

This chapter provides information about the new features introduced in the Cisco IOS XE 3.4S releases. In addition, important notes about these releases are included in this chapter.

Cisco IOS XE 3S releases inherit all Cisco IOS XE Release 2 features that were released prior to the introduction of the Cisco IOS XE 3S releases with few exceptions. For information about inherited features that were introduced in Cisco IOS XE Release 2 releases, for a list of new and changed features, and for important notes that apply to Cisco IOS XE Release 2, see the “New and Changed Information” section in Cisco IOS XE Release 2 Release Notes.

This chapter contains the following sections:

- New and Changed Information, page 91
- Important Notes, page 101

New and Changed Information

The following sections list the new hardware and software features that are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.4S:

- New Hardware Features in Cisco IOS XE Release 3.4.6S, page 92
- New Software Features in Cisco IOS XE Release 3.4.6S, page 92
- New Hardware Features in Cisco IOS XE Release 3.4.5S, page 92
- New Software Features in Cisco IOS XE Release 3.4.5S, page 92
- New Hardware Features in Cisco IOS XE Release 3.4.4S, page 92
- New Software Features in Cisco IOS XE Release 3.4.4S, page 92
- New Hardware Features in Cisco IOS XE Release 3.4.3S, page 92
- New Software Features in Cisco IOS XE Release 3.4.3S, page 92
- New Hardware Features in Cisco IOS XE Release 3.4.2S, page 93
- New Software Features in Cisco IOS XE Release 3.4.2S, page 93
- New Hardware Features in Cisco IOS XE Release 3.4.1S, page 93
New Hardware Features in Cisco IOS XE Release 3.4.6S

There are no new hardware features introduced in Cisco IOS XE Release 3.4.6S.

New Software Features in Cisco IOS XE Release 3.4.6S

There are no new software features introduced in Cisco IOS XE Release 3.4.6S.

New Hardware Features in Cisco IOS XE Release 3.4.5S

There are no new hardware features introduced in Cisco IOS XE Release 3.4.5S.

New Software Features in Cisco IOS XE Release 3.4.5S

There are no new software features introduced in Cisco IOS XE Release 3.4.5S.

New Hardware Features in Cisco IOS XE Release 3.4.4S

There are no new hardware features introduced in Cisco IOS XE Release 3.4.4S.

New Software Features in Cisco IOS XE Release 3.4.4S

There are no new software features introduced in Cisco IOS XE Release 3.4.4S.

New Hardware Features in Cisco IOS XE Release 3.4.3S

There are no new hardware features introduced in Cisco IOS XE Release 3.4.3S.

New Software Features in Cisco IOS XE Release 3.4.3S

The following are the new software features introduced in Cisco IOS XE Release 3.4.3S.

IPv6 ACL Extensions for Hop by Hop Filtering

For detailed information, see the following Cisco document:
New Hardware Features in Cisco IOS XE Release 3.4.2S

There are no new hardware features introduced in Cisco IOS XE Release 3.4.2S.

New Software Features in Cisco IOS XE Release 3.4.2S

There are no new software features introduced in Cisco IOS XE Release 3.4.2S.

New Hardware Features in Cisco IOS XE Release 3.4.1S

There are no new hardware features introduced in Cisco IOS XE Release 3.4.1S.

New Software Features in Cisco IOS XE Release 3.4.1S

There are no new software features introduced in Cisco IOS XE Release 3.4.1S.

New Hardware Features in Cisco IOS XE Release 3.4.0S

Cisco IOS XE Release 3.4.0S supports GLC-ZX-SMD SFP module. For detailed information on the GLC-ZX-SMD SFP module, see the following Cisco document:


New Software Features in Cisco IOS XE Release 3.4.0S

The following are the new software features introduced in Cisco IOS XE Release 3.4.0S.

Application Visibility and Control

For detailed information, see the following Cisco documents:


ASR1K Frame Relay—Multilink (MLFR-FRF.16)

For detailed information, see the following Cisco document:


ASR1K IPSec VPN Scaling Enhancement

In Cisco IOS IOS XE Release 3.4S, IPSec VPN scaling was enhanced as shown in the following table:
New and Changed Information

Maximum Deployable Target (MDT) represents the maximum scaling performance and is achievable only in certain configurations and is supported only for specific configurations and profiles on RP2/ESP20 hardware. The scaling performance may be less on other hardware platforms.

General Deployable Target (GDT), represents the generally applicable scaling performance with common, though not all, feature combinations.

Limitations:
- The maximum number of crypto subinterface, crypto map, crypto spd for site-2-site IPSec is 4,000.
- The maximum IPsec sessions per interface is 4,000.
- At setup time, the tunnels per second (TPS) rate is expected to be lower (about 50 TPS) for high scaling numbers.
- Occasional high CPU usage (>=95%) is observed on both RP and FP when a session establishes at scaling. IKE call admission from 30-50 may help relieve the stress, but this is not guaranteed.
- For dVTI scaling, the ISAKMP in-negotiation-sa CAC should be configured around 30.
- ATM Support for SPA-2CHT3-CE-ATM on ASR1K

For detailed information, see the following Cisco documents:

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Maximum Deployable Target</th>
<th>General Deployable Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>S2S: Static Crypto Map</td>
<td>8,000</td>
<td>8,000</td>
</tr>
<tr>
<td>dVTI</td>
<td>4,000</td>
<td>2,000</td>
</tr>
<tr>
<td>DMVPN/BGP</td>
<td>4,000</td>
<td>4,000</td>
</tr>
<tr>
<td>DMVPN/EIGRP</td>
<td>4,000</td>
<td>4,000</td>
</tr>
</tbody>
</table>

AToM Load Balancing with Single PW

For detailed information, see the following Cisco document:

BFD Support for IP Tunnel (GRE, with IP address)

For detailed information, see the following Cisco document:

BGP Diverse Path Using Diverse-Path-RR

For detailed information, see the following Cisco documents:
BGP Enhanced Route Refresh

For detailed information, see the following Cisco document:

Capabilities Manager

For detailed information, see the following Cisco document:

CEM Support for SPA-24CHT1-CE-ATM on ASR1K

For detailed information, see the following Cisco documents:

Cisco TrustSec SGT Exchange Protocol (SXP) IPv4

For detailed information, see the following Cisco document:

Cisco TrustSec SGT Handling—L2 SGT Imposition and Forwarding

For detailed information, see the following Cisco document:

Domain Stripping at Server Group Level

For detailed information, see the following Cisco document:

Dynamic VTI QoS

For detailed information, see the following Cisco document:
EIGRP Wide Metrics

For detailed information, see the following Cisco document:

ERSPAN Support on Tunnel Interface

In Cisco IOS XE Release 3.4S the following ERSPAN enhancements were added:

- Support was added for the following types of tunnel interface as source ports for a source session:
  - GRE
  - mGRE
  - SVTI
  - PinIP
  - Pv6
  - Pv6 over IP tunnel
    Note that GRE, mGRE, SVTI, and PinIP tunnel interfaces support monitoring of both IPSec protected and non-IPSec protected tunnel packets. This means that you should see the clear-text tunnel packet after IPSec decryption if that tunnel is IPSec protected.
    For IPv6 and IPv6 over IP tunnel interfaces, only monitoring of non-IPSec protected tunnel packets is supported.
- This feature applies only to ERSPAN source sessions, not to ERSPAN destination sessions.
- The tunnel keyword was added to the source interface command.

Cisco IOS XE Release 3.4S introduces the following behavior changes in ERSPAN:

- The tunnel interface is removed from the ERSPAN database at all levels when the tunnel interface is deleted.
  If you want to create the same tunnel again, you must manually configure it in source monitor sessions in order to keep monitoring the tunnel traffic.
- The Layer 2 Ethernet header is feature generated with both source and destination MAC address set to zero.

For detailed information, see the following Cisco document:

EVC MIB

For detailed information, see the following Cisco documents:

FNF—Account on Resolution

For detailed information, see the following Cisco documents:

**FNF—Export on Transaction End**

For detailed information, see the following Cisco documents:

**FNF—Flow-Based Sampling**

For detailed information, see the following Cisco documents:

**FNF—Usage and Transaction Record Support**

For detailed information, see the following Cisco documents:

**GPRS Tunneling Protocol Support**

For detailed information, see the following Cisco document:

**In Service One-Shot Software Upgrade Procedure**

For detailed information, see the following Cisco document:

**IP Multicast Dynamic NAT**

For detailed information, see the following Cisco document:

**IPv4 Loop-Free Alternate Fast-Reroute**

For detailed information, see the following Cisco document:
IPv6 Load Balancing on GEC

For detailed information, see the following Cisco document:

IPv6 Multicast VRF Lite

For detailed information, see the following Cisco document:

IPv6 Virtual Fragmentation Reassembly

For detailed information, see the following Cisco document:

ISG IPv6 Support

For detailed information, see the following Cisco document:

Limiting Resource Usage

For detailed information, see the following Cisco document:

MLP on LNS

For detailed information, see the following Cisco document:

MLPoA and MLPoEoA—PTA

For detailed information, see the following Cisco document:

MLPoE at PTA

For detailed information, see the following Cisco document:

Multicast Service Reflection

For detailed information, see the following Cisco document:
**NBAR Categorization and Attributes**

For detailed information, see the following Cisco documents:


---

**NBAR Classification Enhancements**

For detailed information, see the following Cisco documents:


---

**NBAR Flow Capacity CLI**

For detailed information, see the following Cisco document:


---

**OSPFv2 Loop Free Alternate Fast Reroute**

For detailed information, see the following Cisco document:


---

**OSPFv3 Address Families**

For detailed information, see the following Cisco document:


---

**OSPFv3 External Path Preference Option (RFC 5340 from RFC 2328 16.4.1)**

For detailed information, see the following Cisco document:


---

**OSPFv3 max-metric router-lsa**

For detailed information, see the following Cisco document:


---

**PfR Data Export v1.0 (NetFlow v9 Format)**

For detailed information, see the following Cisco document:
New and Changed Information


**PFR RSVP Control**

For detailed information, see the following Cisco document:

**PFR/RSVP CAC Integration**

For detailed information, see the following Cisco document:

**PIMv6—Anycast RP Solution**

For detailed information, see the following Cisco document:

**Policy Accounting—COA Ordering**

For detailed information, see the following Cisco document:

**Protection Against Distributed Denial of Service Attacks**

For detailed information, see the following Cisco document:

**Proxy Mobile IPv6 Support for MAG Functionality**

For detailed information, see the following Cisco document:

**QoS Demarcation Enhancements**

For detailed information, see the following Cisco document:

**SDP Editing Using Script-Based Editors**

For detailed information, see the following Cisco document:
SRTP Support for RTCP Multiplexed with RTP and for SSRC-Based Multiplexing

For detailed information, see the following Cisco document:

Stateful NAT64 ALG—Stateful FTP64 ALG Support

For detailed information, see the following Cisco document:

Stateful Network Address Translation 64

For detailed information, see the following Cisco document:

Support Termination and Generation of RTCP on DSP SPA

For detailed information, see the following Cisco document:

TFTP IPv6 Support

For detailed information, see the following Cisco document:

Important Notes

The following sections contain important notes about Cisco IOS XE 3S Releases running on Cisco ASR 1000 Series Routers.

Deferrals

Cisco IOS software images are subject to deferral. We recommend that you view the deferral notices at the following location to determine whether your software release is affected:

Field Notices and Bulletins

- Field Notices—We recommend that you view the field notices for this release to determine whether your software or hardware platforms are affected. You can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.
Important Notes About IPSec Support on the Cisco ASR 1000 Series Router

This section contains important notes about IPSec support on the Cisco ASR 1000 Series Router:

**IPSec CLI Support Notes**

This section contains important notes about IPSec CLI support on the Cisco ASR 1000 Series Router.

For information about Cisco IOS IPSec commands, see *Cisco IOS Security Command Reference* at the following location:


- The `show crypto engine` command, which displays information about the crypto engine, is not currently supported on the Cisco ASR 1000 Series Router. The unsupported `show crypto engine` subcommands include the following:
  - `accelerator` (Shows crypto accelerator information.)
  - `brief` (Shows all crypto engines in the system.)
  - `configuration` (Shows crypto engine configuration.)
  - `connections` (Shows connection information.)
  - `qos` (Shows QoS information.)
- The Cisco ASR 1000 Series Router does not currently support the display of send and recv error statistics using the `show crypto ipsec sa identity` command.
- The Cisco ASR 1000 Series Router does not support the `clear` and `show crypto` commands on the standby Route Processor (RP) by design.
- Counters in the `show platform software ipsec fp active flow identifier n` command are flagged for reset on read. You can use the `show crypto ipsec sa` command to obtain integral counters.
- The `show access-list` command output does not show a packet count matching the ACL.
- The Cisco ASR 1000 Series Router displays debugging information about the consumption of IPsec datapath memory; use the `show platform hardware qfp act feature ipsec datapath memory` command in privileged EXEC or diagnostic mode.
- The Cisco ASR 1000 Series Router displays debugging information about the crypto engine processor registers; use the `show platform software ipsec f0 encryption-processor registers` command in privileged EXEC or diagnostic mode.

**IPsec Support on Cisco ASR 1000 Series Routers**

This section contains important notes about IPsec Support on the Cisco ASR 1000 Series Router:

After a rekey or after configuration of an IPsec tunnel, IPsec chunk SPI allocations keep increasing and are not freed until the number of allocations reaches ten. The SPI allocations are freed automatically after the number of allocations reaches ten.

**Crypto Map Support**

This section contains important notes about IPsec crypto map support on the Cisco ASR 1000 Series Router:
Important Notes

The Cisco ASR 1000 Series Router does not currently support IPSec tunnel configuration for crypto maps with same IP address on both the tunnel interface and the physical interface. Configurations with different IP addresses are supported.

A possible Embedded Services Processor (ESP) reload may occur if a large number (such as 2000) of crypto maps are removed simultaneously. When removing a large number of crypto maps, it is recommended you unconfigure 500 crypto maps at a time and wait 25 seconds between operations.

The Cisco ASR 1000 Series Router does not support the `show access-lists id` command under crypto maps.

The Cisco ASR 1000 Series Router does not currently support the `interface range` command when configuring crypto maps.

IPSec Packet Processing
This section contains important notes about IPSec packet processing on the Cisco ASR 1000 Series Router:

- Reloading an Embedded Services Processor (ESP) on the Cisco ASR 1000 Series Router may cause a few IPSec packets to drop before the initialization completes, but the traffic will resume after a brief interval.
- The Cisco ASR 1000 Series Router will not discard an incoming IP datagram containing a Payload Length other than 4 in the authentication header (AH). For example, a 96 bit authentication value plus the 3 32-bit word fixed portion for any non-null authentication algorithm will not be discarded.
- The Cisco ASR 1000 Series Router does not forward incoming authenticated packets with the IP option field set.

GET VPN Support
This section contains important notes about Group Encrypted Transport VPN (GET VPN) support on the Cisco ASR 1000 Series Router:

- To ensure normal traffic flow for a GET VPN configuration on a Cisco ASR 1000 Series Router, a Time Based Anti Replay (TBAR) window-size of greater than 42 seconds is recommended.
- The Cisco ASR 1000 Series Router does not currently support the TBAR statistics display in the `show crypto gdoi gm replay` command.
- The Cisco ASR 1000 Series Router does not currently support Easy VPN (EzVPN) and GET VPN on the same interface.
- When a Cisco ASR 1000 Series Router is to apply the same Group Domain of Interpretation (GDOI) crypto maps to two interfaces, you should use local addresses for the crypto maps. Non-local address configuration is not supported.
- The Cisco ASR 1000 Series Router does not currently support transport mode for TBAR.
- The Cisco ASR 1000 Series Router only supports the reassembly of post-fragmented GET VPN packets that are destined for the local Cisco ASR 1000 Series Router in the GET VPN network.
- An enhancement is added to enable reassembly of IPsec transit traffic. This enhancement applies only to post-encryption fragmented IPsec packets. When this enhancement is enabled, IPsec will detect transit IPsec traffic and reassemble it before decryption. GET VPN transit IPsec traffic will be reassembled, decrypted, and forwarded to the destination. Non GET VPN transit IPsec traffic will be reassembled but not decrypted (because the Cisco ASR 1000 router is not the IPsec tunnel end point) and then forwarded to the destination.

To enable IPsec reassembly of transit traffic, use the `platform ipsec reassembly transit` command in global configuration mode. To disable IPsec reassembly of transit traffic, use the `no` form of this command.
platform ipsec reassembly transit
[no] platform ipsec reassembly transit

IPSec SSO and ISSU Support Notes

- The Cisco ASR 1000 Series Router supports stateful IPSec sessions on ESP switchover. During ESP switchover, all IPSec sessions will stay up and no user intervention is needed to maintain IPSec sessions.

- For an ESP reload (no standby ESP), the SA sequence number restarts from 0. The peer router drops packets that do not have the expected sequence number. User may need to explicitly reestablish IPSec sessions to work around this issue for systems that have a single ESP after an ESP reload. User may experience traffic disruption over the IPSec sessions in such cases for the duration of the reload.

- The Cisco ASR 1000 Series Router currently does not support Stateful Switchover (SSO) IPSec sessions on Route Processors (RPs). The IPSec sessions will go down on initiation of the switchover, but will come back up when the new RP becomes active. No user intervention is needed. User will experience traffic disruption over the IPSec sessions for the duration of the switchover, until the sessions are back up.

- The Cisco ASR 1000 Series Router currently does not support stateful ISSU for IPSec sessions. Before performing an ISSU, users must explicitly terminate all existing IPSec sessions or tunnels prior to the operation and reestablish them post ISSU. Specifically, users must ensure that there are no half-open or established IPSec tunnels present before performing ISSU. To do this, we recommend user do a interface shutdown in the case of interfaces that may initiate a tunnel setup, such as a routing protocol initiating a tunnel setup, or interfaces that have keepalive enabled or where there is an auto trigger for an IPSec session. Traffic disruption over the IPSec sessions during ISSU is obvious in this case.

Summarizing Caveats

- ESP—Switchover (with standby ESP): Stateful: IPSec sessions should be up. No user intervention needed.

- ESP—Reload (no standby ESP): Stateless: IPSec sessions will go down and come back. Usually, no user intervention is needed. However, users may have to explicitly re-establish an IPSec session if antireplay is configured (sequence number checking).

- RP—Switchover (with standby RP): Stateless: IPSec sessions will go down on RP switchover and the session should re-establish automatically when the new RP gains an active role. No user intervention is needed.

- ISSU (irrespective of chassis type): Stateless: Users must explicitly terminate all the IPSec sessions by shutting the interfaces, perform ISSU, and then re-establish tunnels by enabling the interfaces. No other intervention is needed.

Miscellaneous IPSec Support Notes

This section contains miscellaneous important notes about IPSec support on the Cisco ASR 1000 Series Router:

- In the context of an IPSec DVTI connection, the Cisco ASR 1000 Router does not support dynamic download ACL rule (per-user attribute) from the AAA server.

For example, the following configurations are not supported:

cisco-avpair += "ip:inacl#1=permit ip any 2.2.2.0 0.0.0.255"
cisco-avpair += "ip:outacl#1=permit ip 2.2.2.0 0.0.0.255 any"
The Cisco ASR 1000 Router does not support the command of “if-state nhrp” in configuring the tunnel.

The Cisco ASR 1000 Router Dead Peer Detection behavior is different than the pre-defined behavior (i.e. when there is no traffic to be sent, no DPD is sent, while if any traffic to be sent, DPD is sent). A Cisco ASR 1000 Router DPD is sent out regardless there is outbound traffic needs to be sent out.

The Cisco ASR 1000 Router does not support SA Path MTU on data path.

The Cisco ASR 1000 Router does not support double ACL in dynamic crypto map.

VRF without crypto map configured on a physical interface causes dual esp reload on a Cisco ASR 1000 Router.

The command: `show crypto ipsec sa identity` does not log send and receive error counts.

The commands: `clear crypto` and `show crypto` on Standby RP are inconsistent with Active RP. At present most of other features disable 'clear commands' from Standby RP, but IPSec still allows to clear sa, session etc. from the standby.

The Cisco ASR 1000 Router does not support Cisco AAA av-pair “cisco-avpair += ip:sub-policy-In=policy1”.

CLI allows both ikev1 and ikev2 profile configured under the same crypto map, even though it is not supported internally on the ASR 1000 Router.

For a Cisco ASR 1000 Router, the tunnel protection should be removed first before changing any configuration for tunnel protection.

The security association (SA) maximum transmission unit (MTU) calculation is based on the interface MTU instead of the IP MTU.

The Cisco ASR 1000 Series Router currently supports a maximum anti-replay window value of 512. If you attempt to configure a value larger than 512, the Cisco ASR 1000 Series Router defaults back to 512 internally (although the display still shows your user-configured value).

The Cisco ASR 1000 Series Router does not currently support nested SA transformation such as:

```
crypto ipsec transform-set transform-1 ah-sha-hmac esp-3des esp-md5-hmac
crypto ipsec transform-set transform-1 ah-md5-hmac esp-3des esp-md5-hmac
```

The Cisco ASR 1000 Series Router does not currently support Cisco IOS Certificate Authority (CA) server features.

The Cisco ASR 1000 Series Router does not currently support COMP-LZS configuration.

On Cisco ASR 1000 Series Routers, when configuring GRE over IPSec, it is recommended that you use only the tunnel protection mode on the tunnel interface. Using crypto maps on both the tunnel interface and the physical interface to achieve GRE over IPSec is not the supported method of configuration.

When using dynamic VTI-based IPSec on a Cisco ASR 1000 Router, if there are multiple remote IPSec endpoints behind the same NAT device, only one of the endpoints has connectivity. In other words, multiple endpoints cannot have connectivity at the same time.

**NAT and Firewall ALG Support on the Cisco ASR 1000 Series Routers**

*NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers* matrix summarizes Network Address Translation (NAT) and Firewall Application Layer Gateway (ALG) feature support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1.0 and later releases. The matrix lists feature support by release. NAT and Firewall ALG support is cumulative; features introduced in earlier releases continue to be supported in later releases. You can find the matrix at the following location:
Important Notes About Cisco IOS XE Release 3.4.1S

This section provides important notes about Cisco IOS XE Release 3.4.1S.

BGP Scan Time Range

The `bgp scan-time` command has a scanner-interval range of 5-60 seconds. The `bgp scan-time` command can be configured, even if BGP Next Hop Tracking (NHT) is configured (by the `bgp nexthop` command).

Important Notes About Cisco IOS XE Release 3.3.1S

This section provides important notes about Cisco IOS XE Release 3.3.1S.

Broadband Encapsulation Autosense Support Notes

This section contains important notes about the support for broadband encapsulation autosense with RBE configuration in Cisco IOS XE Release 3.3.1S:

- The broadband encapsulation autosense enhancement enables broadband autosense support for PPPoEoA, PPPoA, and RBE.
- In the Cisco IOS XE releases prior to Release 3.3.1S, aal5autoppp encapsulation was not supported when an RBE was configured. As a result, the combination of aal5autoppp encapsulation with RBE was not supported in the Cisco IOS XE releases prior to Release 3.3.1S.
- The broadband encapsulation enhancement in Cisco IOS XE Release 3.3.1S supports the combination of aal5autoppp encapsulation with RBE-related configurations.

Important Notes About Cisco IOS XE Release 3.3.0S

This section provides important notes about Cisco IOS XE Release 3.3.0S and later releases.

High Availability on SBC

The following is the expected behavior of a session border controller (SBC) on which the High Availability feature is configured:

If switchover occurs while an H.323–H.323 T.38 fax transmission is in progress, the call does not fall back to the voice mode after the completion of the fax transmission. This is because the signaling state is not preserved in the event of a switchover.
**IPsec Failover**

IPSec failover is a feature that increases the total uptime (or availability) of your IPSec network. Traditionally, this is accomplished by employing a redundant (standby) router in addition to the original (active) router. If the active router becomes unavailable for any reason, the standby router takes over the processing of IKE and IPSec.

IPSec failover falls into two categories: stateless failover and stateful failover. The IPSec on the Cisco ASR 1000 Series Router supports only stateless failover. Stateless failover uses protocols such as the Hot Standby Router Protocol (HSRP) to provide primary to secondary cutover and also allows the active and standby VPN gateways to share a common virtual IP address.

**Important Notes About Cisco IOS XE Release 3.2.1S**

This section describes important notes about Cisco IOS XE Release 3.2.1S and later releases.

**EzVPN Support on Cisco ASR 1000 Series Routers**

On an ASR Cisco 1000 Router, when an EzVPN session is ended, the EzVPN server sends out a Stop Accounting message. This message does not contain the Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, and Acct-Output-Packets fields. It might cause a disruption of accounting performed on traffic.

**Maximum IP MTU for Loopback Interfaces**

For loopback interfaces, the maximum IP MTU is now 4000. This is to match the serial interface limits.

**Important Notes About Cisco IOS XE Release 3.2.0S**

This section describes important notes about Cisco IOS XE Release 3.2.0S and later releases.

**Cisco ASR 1001-4XT3**

Cisco ASR1001-4XT3 chassis functionality is similar to the SPA-4XT3/E3 with the exception of E3 circuitry in Cisco IOS XE 3.2.0S Release.

**SIP Trunk Over TCP**

SIP TCP trunk calls may not activate if more than one complete SIP messages were contained in one TCP segment in Cisco IOS XE 3.2.0S Release.

This symptom occurs upon SIP trunk over TCP scenario. SIP ALG currently processes only one complete SIP message in one TCP segment (one complete or one complete plus one incomplete), refer to CSCti56370.
TCP Failover in Hardware High-Availability Mode

TCP failover is not supported in Hardware High-Availability mode. If the active node fails in Hardware High Availability mode and if the network is restored, it may take 5 to 10 minutes for the standby node to become the active node. This is because of the reboot and the peer negotiation delay. If the network is not restored, only the switched over active peer is available. Failover is not possible in this state.

Extended ACL as a WCCP Redirect ACL

The Cisco ASR 1000 Series Router supports the use of an extended ACL as a WCCP redirect ACL. However, the option to specify a port range is not supported.

Important Notes About Cisco IOS XE Release 3.1.1S

This section describes important notes about Cisco IOS XE Release 3.1.1S and later releases.

SIP-40G:SPA-4XT-SERIAL

Cisco SPA-4XT-SERIAL was not supported in 3.1.0S when plugged into an ASR1000 with SIP-40. This SPA is supported in Release 3.1.1S on SIP-40 linecard.

For more information, see the following documents:
Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation, see section for SPA-4XT-Serial in Table 1-4 (SIP and SPA Compatibility for Serial SPAs).
Cisco ASR1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide

Important Notes About Cisco IOS XE Release 3.1.0S

This section describes important notes about Cisco IOS XE Release 3.1.0S and later releases.

Bidirectional Forwarding Detection (BFD)

In Cisco IOS XE Release 3.1.0S, Bidirectional Forwarding Detection (BFD) is no longer supported in IP Base software packages. For BFD support, use the Advanced IP Services or Advanced Enterprise Services packages.

DMVPN Spoke Support

In Cisco IOS XE Release 3.1.0S Cisco ASR 1000 Series Routers do not support the ip nhrp server-only command if they act as DMVPN spokes.
Important Notes About Cisco IOS XE Release 2.6.0

This section describes important notes about Cisco IOS XE Release 2.6.0 and later releases.

Per-User Attribute on PPP Virtual Access

In Cisco IOS XE Release 2.6.0 multiple instances of the per-user attribute ‘Cisco-Avpair=lcp:interface-config=\<cmd\>’ is not supported.

For example:
Cisco-AVPair = lcp:interface-config=ip vrf forwarding vpngreen
Cisco-AVPair= lcp:interface-config=ip unnumbered loopback2
Should be configured like this in Cisco IOS XE Release 2.6.0:
Cisco-AVPair = lcp:interface-config=ip vrf forwarding vpngreen \ip unnumbered loopback2
“Multiple instances will be supported in Cisco IOS XE Release 2.6.1”

Legacy QoS Command Deprecation: Hidden Commands

To streamline Cisco IOS QoS (quality of service), certain commands are being hidden. Although these commands are available in Cisco IOS XE Release 2.6, the CLI interactive help does not display them. If you attempt to view a command by entering a question mark at the command line, the command does not appear. However, if you know the command syntax, you can enter it. The system will accept the command and return a message explaining that it will soon be removed. These commands will be completely removed in a future release, which means that you will need to use the appropriate replacement commands.

For more information, see the following document:

VRF-Aware NAT

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.5.0

This section describes important notes about Cisco IOS XE Release 2.5.0 and later releases.

Embedded Packet Capture

The Embedded Packet Capture (EPC) feature is not functional and not supported for the Cisco ASR 1000 Series Routers.
Important Notes

QoS: Policing Support for GRE Tunnels

When queuing feature on the GRE tunnel interface is not supported with crypto configured on the physical interface.

QoS: Support for GRE/sVTI Tunnel

With IOS XE 2.5.0, the Cisco ASR 1000 Router Series supports Quality-of Service (QoS) applied to

- A GRE or sVTI tunnel with policing and marking only for INGRESS traffic
- A GRE or sVTI tunnel with 2-level hierarchy allowing queuing on the second level for EGRESS traffic

When there are multiple egress physical interfaces for a tunnel, and the tunnel target physical interface changes as a result of tunnel target destination route change, either manually by user configuration or by routing protocol, IOS will not prevent the tunnel traffic from moving to an alternate egress physical interface. However, in IOS XE 2.5.0, QoS tunnel move feature is not supported. When tunnel traffic moved to an alternate egress physical interface, tunnel QoS policy may enter a suspended state. At this point, the tunnel QoS policy will have to be removed and reapplied to the tunnel interface for it to take effect. In addition, queuing features on the GRE tunnel interface are not supported when IPSec is configured on the physical interface.

VRF-Aware NAT

Integrating NAT with MPLS VPNs

This section provides information about integrating NAT with MPLS VPNs.

Prerequisites for Integrating NAT with MPLS VPNs

Before performing the tasks in this module, you should be familiar with the concepts related to configuring NAT for IP address conservation. All access lists required for use with the tasks in this module should be configured prior to beginning the configuration task. For information about how to configure an access list, see IP Access List Sequence Numbering at the following location:


Note: If you specify an access list to use with a NAT command, NAT does not support the commonly used permit ip any command in the access list.

Restrictions for Integrating NAT with MPLS VPNs

- The following functionality is not supported for VRF-Aware NAT:
  - VPN to VPN translations. In other words, VRF cannot be applied on the NAT outside interface.
  - Translation of multicast packets
  - Translations with inside destinations
  - Reversible route maps
  - MIBs
  - MPLS traffic engineering
- Configuring inside dynamic translations defined with outside interface mappings is not supported.
• Configuring inside static translations with interface mappings is not supported. The following commands, which do not include VRF, are not supported:
  – `ip nat inside source static esp local-ip interface type number`
  – `ip nat inside source static local-ip global-ip route-map name`
  – `ip nat inside source static local-ip interface type number`
  – `ip nat inside source static tcp local-ip local-port interface type number global-port`
  – `ip nat inside source static udp local-ip local-port interface type number global-port`

Dependency of NAT on VFR
ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.3.0
This section describes important notes about Cisco IOS XE Release 2.3.0 and later releases.

Any Transport Over MPLS (AToM) Support
The configuration of Any Transport Over MPLS (AToM) on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.3.0 is only supported on a subinterface; AToM cannot be configured on the main interface. In addition, you cannot have any IP configuration on the main interface when you have an AToM configuration on the subinterface. These configuration guidelines are applicable to VC mode, VP mode, and L2VPN PW redundancy.

MPLS TE Support
Cisco ASR 1000 Series Router users considering the implementation of MPLS TE are recommended to consult with their local Cisco technical support representative for Cisco IOS XE implementation details.

VRF-Aware NAT

Dependency of NAT on VFR
ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.2.2
This section describes important notes about Cisco IOS XE Release 2.2.2 and later releases.

SSO for L2TP Tunnel Switching Not Supported
If dual route processors (RPs) are used on the Cisco ASR 1000 Series Router in Cisco IOS XE Release 2.2.2 and L2TP Tunnel Switching is configured, then `no l2tp sso enable` must be configured.
Important Notes About Cisco IOS XE Release 2.2.1

This section describes important notes about Cisco IOS XE Release 2.2.1 and later releases.

100M FX SFP Not Supported on Cisco 2-Port Gigabit Ethernet Shared Port Adapter

The 100M FX SFP is not supported on the Cisco 2-Port Gigabit Ethernet Shared Port Adapter (2x1GE SPA) on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2.1.

Intelligent Service Gateway (ISG) Features Not Supported

The following Intelligent Service Gateway (ISG) features are not supported on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2.1:

- ISG IP subscriber functionality on the following types of access interfaces: Gigabit EtherChannel (GEC) (Port Channel), generic routing encapsulation (GRE), PPP (virtual-template), and Layer 2 Tunneling Protocol (L2TP)
- ISG prepaid billing
- ISG IP interface sessions
- Interface statistics for ISG multiservice interfaces
- Access lists cannot be configured as match criteria in ISG Layer 4 redirect configuration. As an alternative, Layer 4 redirect should be configured in ISG traffic class services.
- Stateful Switchover (SSO and in-service software upgrade (ISSU) for ISG IP subscriber sessions or traffic class sessions. Upon switchover, an IP session must be recreated or restarted (for Dynamic Host Configuration Protocol (DHCP) sessions) when the session becomes active again.
- SSO and ISSU for any features on IP subscriber sessions or traffic class sessions
- SSO and ISSU for the following features on ISG PPP sessions:
  - Port-Bundle Host Key
  - Layer 4 Redirect
  - Traffic Class

Per-Session Multicast Support

Enhancements to the IP multicast feature provide support for per-session multicast in broadband environments in Cisco IOS XE Release 2.2.1.
VRF-Aware NAT

Dependency of NAT on VFR

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces and environments in Cisco IOS XE Release 2.2.1. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.1.1

This section describes important notes about Cisco IOS XE Release 2.1.1 and later releases.

Startup Configuration File Backup

As a matter of routine maintenance on any Cisco router, users should backup the startup configuration file by copying the startup configuration file from NVRAM onto one of the router’s other file systems and, additionally, onto a network server. Backing up the startup configuration file provides an easy method of recovering the startup configuration file in the event the startup configuration file in NVRAM becomes unusable for any reason.

For users using any Cisco ASR 1000 Series Router with a single RP, including any Cisco ASR 1002 or Cisco ASR 1004 Router, backing up the startup configuration file onto another router file system is especially important due to CSCsq70140, which is documented in the Caveats section of these release notes. The workaround for users who run into this caveat is to replace the startup configuration file in NVRAM with a backup copy of the startup configuration file on the router; therefore, customers who have backed up their startup configuration files onto the router will be ready to resolve these caveats if they occur on their Cisco ASR 1000 Series Routers using a single RP.

Example 1: Copying Startup Configuration File to Bootflash

Router# dir bootflash:
Directory of bootflash/

    11  drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
    86401  drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
   14401  drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
   28801  drwx 4096 May 29 2008 16:31:41 -07:00 .prst_sync
   43201  drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
         12 -rw- 208904396 May 28 2008 16:17:34 -07:00
asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin

Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]?

3517 bytes copied in 0.647 secs (5436 bytes/sec)

Router# dir bootflash:
Directory of bootflash/

    11  drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
    86401  drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
   14401  drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
   28801  drwx 4096 May 29 2008 16:31:41 -07:00 .prst_sync
   43201  drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
         12 -rw- 208904396 May 28 2008 16:17:34 -07:00
asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin
Example 2: Copying Startup Configuration File to USB Flash Disk

Router# dir usb0:
Directory of usb0:/

43261 -rwx 208904396 May 27 2008 14:10:20 -07:00 asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin
255497216 bytes total (40190464 bytes free)

Router# copy nvram:startup-config usb0:
Destination filename [startup-config]?

3172 bytes copied in 0.214 secs (14822 bytes/sec)

Router# dir usb0:
Directory of usb0:/

43261 -rwx 208904396 May 27 2008 14:10:20 -07:00 asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin
43262 -rwx 3172 Jul 2 2008 15:40:45 -07:00 startup-config

255497216 bytes total (40186880 bytes free)

Example 3: Copying Startup Configuration File to a TFTP Server

Router# copy bootflash:startup-config tftp:
Address or name of remote host [1]? 172.17.16.81
Destination filename [pe24_asr-1002-conf]? /auto/tftp-users/user/startup-config
3517 bytes copied in 0.122 secs (28828 bytes/sec)

VRF-Aware NAT

Dependency of NAT on VFR
ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.1.0

This section describes important notes about Cisco IOS XE Release 2.1.0 and later releases.

High-Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers

Table 1 describes some of the high level feature sets that are not supported for the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1.0 and later releases. Use Cisco Feature Navigator to confirm support for a specific feature. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Feature support is subject to change from release to release. Some high-level feature sets that were not supported in the initial Cisco IOS XE Release 2.1.0 are now supported. Table 1 has been updated to indicate when support has been introduced in later releases. For the latest feature information, see the New and Changed Information sections of these release notes and Cisco Feature Navigator.

### Table 1  High-Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers

<table>
<thead>
<tr>
<th>Major Feature Category</th>
<th>Features Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ATM</strong></td>
<td>Support for ATM features begins in Cisco IOS XE Release 2.3.0. No ATM features are supported in earlier releases.</td>
</tr>
<tr>
<td><strong>Broadband</strong></td>
<td>Support for ANCP begins in Cisco IOS XE Release 2.4.0. ANCP is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>IPv6 Intelligent Service Gateway (IPv6 ISG)</td>
</tr>
<tr>
<td></td>
<td>Point-to-Point Protocol over Ethernet Tag (PPPoE Tag)</td>
</tr>
<tr>
<td></td>
<td>PPP over Q-in-Q (PPPoQinQ)</td>
</tr>
<tr>
<td><strong>Ethernet OAM</strong></td>
<td>Ethernet Operation, Administration, and Maintenance (OAM)</td>
</tr>
<tr>
<td><strong>MPLS</strong></td>
<td>Support for Carrier’s Carrier begins in Cisco IOS XE Release 2.2.3. Carrier’s Carrier is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>Support for Ethernet over MPLS (EoMPLS) begins in Cisco IOS XE Release 2.4.0. Ethernet over MPLS (EoMPLS) is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>Support for Inter-AS begins in Cisco IOS XE Release 2.2.2. Inter-AS is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>IPv6 Provider Edge Router over MPLS (6PE)</td>
</tr>
<tr>
<td></td>
<td>IPv6 VPN over MPLS (6VPE)</td>
</tr>
<tr>
<td></td>
<td>Label Distribution Protocol (LDP) Session Protection</td>
</tr>
<tr>
<td></td>
<td>Support for Layer 2 VPN (L2VPN) begins in Cisco IOS XE Release 2.3.0. L2VPN is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>Support for MPLS Traffic Engineering/Fast Reroute (MPLS TE/FRR) begins in Cisco IOS XE Release 2.3.0. MPLS TE/FRR is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>Virtual Private LAN Service (VPLS)</td>
</tr>
<tr>
<td><strong>Multicast</strong></td>
<td>Multicast VPN</td>
</tr>
<tr>
<td><strong>Routing</strong></td>
<td>Performance Routing/Optimized Edge Routing (PFR/OER)</td>
</tr>
</tbody>
</table>
### Important Notes

**Security**
- Support for Group Encrypted Transport VPN (GET VPN) begins in Cisco IOS XE Release 2.3.0. GET VPN is not supported in earlier releases.
- IPv6 IPSec
  - Support for Lawful Intercept begins in Cisco IOS XE Release 2.4.0. Lawful Intercept is not supported in earlier releases.
- VRF-Aware Firewall
  - Support for VRF-Aware NAT when running ASRNAT this will not handle fragmented packets unless VFR is configured on all NAT interfaces.

**Voice**
- Support for Cisco Unified Border Element (SP Edition) begins in Cisco IOS XE Release 2.4.0. Cisco Unified Border Element (SP Edition) is not supported in earlier releases. Earlier releases include support for Integrated Session Border Controller.

---

**Table 1**  
*High-Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers (continued)*

<table>
<thead>
<tr>
<th>Major Feature Category</th>
<th>Features Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Support for Group Encrypted Transport VPN (GET VPN) begins in Cisco IOS XE Release 2.3.0. GET VPN is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>IPv6 IPSec</td>
</tr>
<tr>
<td></td>
<td>Support for Lawful Intercept begins in Cisco IOS XE Release 2.4.0. Lawful Intercept is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>VRF-Aware Firewall</td>
</tr>
<tr>
<td></td>
<td>Support for VRF-Aware NAT when running ASRNAT this will not handle fragmented packets unless VFR is configured on all NAT interfaces.</td>
</tr>
<tr>
<td>Voice</td>
<td>Support for Cisco Unified Border Element (SP Edition) begins in Cisco IOS XE Release 2.4.0. Cisco Unified Border Element (SP Edition) is not supported in earlier releases. Earlier releases include support for Integrated Session Border Controller.</td>
</tr>
</tbody>
</table>
New Features in and Important Notes About Cisco IOS XE 3.3S Releases

This chapter provides information about the new features introduced in the Cisco IOS XE 3.3S releases. In addition, important notes about these releases are included in this chapter.

Cisco IOS XE 3S releases inherit all Cisco IOS XE Release 2 features that were released prior to the introduction of the Cisco IOS XE 3S releases with few exceptions. For information about inherited features that were introduced in Cisco IOS XE Release 2 releases, for a list of new and changed features, and important notes that apply to Cisco IOS XE Release 2, see the “New and Changed Information” section in Cisco IOS XE Release 2 Release Notes.

This chapter contains the following sections:
- New and Changed Information, page 117
- Important Notes, page 128

New and Changed Information

The following sections list the new hardware and software features that are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.3S:
- New Hardware Features in Cisco IOS XE Release 3.3.2S, page 117
- New Software Features in Cisco IOS XE Release 3.3.2S, page 118
- New Software Features in Cisco IOS XE Release 3.3.1S, page 118
- New Hardware Features in Cisco IOS XE Release 3.3.0S, page 118
- New Software Features in Cisco IOS XE Release 3.3.0S, page 119

New Hardware Features in Cisco IOS XE Release 3.3.2S

No new hardware features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.3.2S.
New Software Features in Cisco IOS XE Release 3.3.2S

No new software features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.3.2S.

New Hardware Features in Cisco IOS XE Release 3.3.2S

No new hardware features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.3.1S.

New Software Features in Cisco IOS XE Release 3.3.1S

No new software features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.3.1S.

New Hardware Features in Cisco IOS XE Release 3.3.0S

The following are new hardware features introduced in Cisco IOS XE Release 3.3.0S:

8-Port Integrated Daughter Card (IDC-CHT1/E1) for the Cisco ASR 1001 Router

For detailed information, see the following Cisco document:

CEM Support for SPA-1CHOC3-CE-ATM

For detailed information, see the following Cisco documents:

Gigabit Ethernet Integrated Daughter Card (IDC-4XGE) for the Cisco ASR 1001 Router

For detailed information, see the following Cisco document:

Hard Disk Drive Integrated Daughter Card (IDC-HD80G) for the Cisco ASR 1001 Router

For detailed information, see the following Cisco document:
SPA-1X10GE-WL-V2 SPA Support

For detailed information, see the following Cisco documents:

Support for the Cisco ASR 1013 Router Power Supplies on the Cisco ASR 1006 Router

For detailed information, see the following Cisco document:

New Software Features in Cisco IOS XE Release 3.3.0S

The following are new software features introduced in Cisco IOS XE Release 3.3.0S:

ACL and QoS Enhancements to EVC Infrastructure in Cisco IOS XE Software

This feature supports Layer 3 and Layer 4 ACL and QoS on Ethernet service instances (also called Ethernet flow points). Specifically, the following ACL functions are supported:
- Standard ACLs—Both numbered and named
- Extended ACLs—Both numbered and named
- Protocol filtering
- TCP and UDP ports—Less than, greater than, equal to, and negative ranges
In addition, the following QoS functions are supported:
- H-QoS
- Layer 2 classification—VLAN and CoS, both outer and inner
- Layer 3 classification—IP precision and DSCP
- Marking—CoS (inner and outer), IP precision, DSCP, and QoS group
- Policing—1R2C and 2R3C
- Queuing—Priority queuing, WRED, and bandwidth sharing
For detailed information, see the following Cisco documents:

ATM Cell Loss Priority (CLP) Setting

For detailed information, see the following Cisco document:
New and Changed Information

ATM Hierarchical Shaping: ATM VC into VP Shaping

For detailed information, see the following Cisco document:

Autosense of MUX/SNAP Encapsulation and PPPoA or PPPoE on ATM PVCs

For detailed information, see the following Cisco document:

BFD—RIPv2 Support

For detailed information, see the following Cisco document:

BGP Consistency Checker

For detailed information, see the following Cisco document:

BGP IPv6 Client for Single-Hop BFD

For detailed information, see the following Cisco document:

BGP IPv6 PIC Edge and Core for IP/MPLS

For detailed information, see the following Cisco document:

BGP Route Server

For detailed information, see the following Cisco document:

Cisco Unified Border Element (SP Edition)—BFCP Over UDP Support

For detailed information, see the following Cisco document:
Cisco Unified Border Element (SP Edition)—General Enhancements

For detailed information, see the following Cisco document:

EasyVPN Phase 7

For detailed information, see the following Cisco document:

Embedded Event Manager (EEM) 3.2

For detailed information, see the following Cisco document:

Firewall Resource Management

For detailed information, see the following Cisco document:

Firewall TCP SYN Cookie

For detailed information, see the following Cisco document:

Flexible NetFlow—IPv6 Unicast Flows

For detailed information, see the following Cisco document:

Flexible NetFlow—ISSU/SSO Support

For detailed information, see the following Cisco documents:

H.323 to H.323 Video Support with HA

For detailed information, see the following Cisco document:
New Features in and Important Notes About Cisco IOS XE 3.3S Releases

**New and Changed Information**

**IKEv2—Site to Site**

For detailed information, see the following Cisco document:


**Interchassis High Availability Support on the Cisco ASR 1006 Router and the Cisco ASR 1013 Router for Firewall, NAT, and CUBE(SP)**

For detailed information, see the following Cisco document:


**Introduction of New MIBs**

The following MIBs have been introduced in this release:

- CISCO-ENTITY-PERFORMANCE-MIB
- CISCO-SESS-BORDER-CTRLR-STATS-MIB
- ETHER-WIS

For detailed information, see the following Cisco document:


**IPv6 Access Services—PPPoA**

For detailed information, see the following Cisco document:


**IPv6 Dual Stack**

For detailed information, see the following Cisco document:


**ISSU—PPPoA**

For detailed information, see the following Cisco document:


**L2VPN Interworking**

For detailed information, see the following Cisco documents:

http://www.cisco.com/go/cfn
L2VPN Interworking—Ethernet VLAN to ATM AAL5

For detailed information, see the following Cisco documents:

L2VPN Interworking—Ethernet VLAN to Frame Relay

For detailed information, see the following Cisco document:

L2VPN Interworking—Ethernet VLAN to PPP

For detailed information, see the following Cisco document:

L2VPN Pseudowire Redundancy for L2TPv3

For detailed information, see the following Cisco document:

Layer 2 Local Switching—ATM to ATM

For detailed information, see the following Cisco documents:

Layer 2 Tunneling Protocol (L2TP)

For detailed information, see the following Cisco document:

HDLC over Layer 2 Tunneling Protocol Version 3 (L2TPv3)

For detailed information, see the following Cisco document:

LISP Locator/ID Separation Protocol

For detailed information, see the following Cisco document:
MIB for IEEE 1588-2008 Timing Services

The IEEE 1588-2008 standard defines a protocol that enables precise synchronization of clocks in measurement and control systems implemented with packet-based networks. This MIB supports the Precision Time Protocol version 2 (PTPv2) features of Cisco devices.

MIB Support for the Cisco ASR 1001 Router

For detailed information, see the following Cisco document:

MIB Support for SPA-1CHOC3-CE-ATM and SPA-1X10GE-WL-V2

For detailed information, see the following Cisco document:

MPLS TE over GRE Tunnel Support

For detailed information, see the following Cisco document:

NBAR PDL

For detailed information, see the following Cisco document:

NBAR Port-Based Classification for IPv6

For detailed information, see the following Cisco document:

NBAR Protocol Pack

For detailed information, see the following Cisco document:

OSPF—Nonstop Routing

For detailed information, see the following Cisco document:

OSPF Support for NSSA RFC 3101

For detailed information, see the following Cisco document:
Per User AAA Policy Download with PKI

For detailed information, see the following Cisco document:

PfR Master Controller Support

For detailed information, see the following Cisco documents:

PPP over ATM

For detailed information, see the following Cisco documents:

PPPoA or PPPoE Autosense for ATM PVCs

For detailed information, see the following Cisco document:

QoS—Set ATM CLP Bit Using Policer

For detailed information, see the following Cisco document:

Remote Access MPLS—VPN

For detailed information, see the following Cisco document:

RSVP Agent

For detailed information, see the following Cisco document:

show cli Command to Display CUBE-Related Information

For detailed information, see the following Cisco document:
show packet match statistics Command for QoS

For detailed information, see the following Cisco document:

Show QoS Packet Marking Statistics

For detailed information, see the following Cisco document:

SIP Loopback Support

For detailed information, see the following Cisco document:

SIP-SIP Basic Feature Functionality for Session Border Controller (SBC)

For detailed information, see the following Cisco document:

SIP-SIP Extended Feature Functionality for Session Border Controller (SBC)

For detailed information, see the following Cisco document:

SIP Video Support for Telepresence Calls

For detailed information, see the following Cisco document:

SSO—PPPoA

For detailed information, see the following Cisco document:

Support for Call Routing Logic in the Cisco Unified Border Element Based on the Information Embedded in the History-info Header

For detailed information, see the following Cisco documents:
Support for Hiding the Internal Topology Information Embedded Within the History-info Header in
the Cisco Unified Border Element

For detailed information, see the following Cisco documents:

Support for Reporting End-of-Call Statistics in SIP BYE Message

For detailed information, see the following Cisco documents:

Unified Communications Trusted Firewall Control

For detailed information, see the following Cisco documents:

Unified Communications Trusted Firewall Control—Version 2

For detailed information, see the following Cisco documents:

Videoconferencing for the Cisco Multiservice IP-to-IP Gateway Feature

For detailed information, see the following Cisco documents:

VRF-Aware H.323 and SIP

For detailed information, see the following Cisco document:

VRF-Aware NBAR

For detailed information, see the following Cisco document:
VRF-Aware Software Infrastructure (VASI) Scale

For detailed information, see the following Cisco document:


Important Notes

The following sections contain important notes about Cisco IOS XE 3S Releases running on Cisco ASR 1000 Series Routers.

Deferrals

Cisco IOS software images are subject to deferral. We recommend that you view the deferral notices at the following location to determine whether your software release is affected:


Field Notices and Bulletins

- Field Notices—We recommend that you view the field notices for this release to determine whether your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Important Notes About IPSec Support on the Cisco ASR 1000 Series Router

This section contains important notes about IPSec support on the Cisco ASR 1000 Series Router:

IPSec CLI Support Notes

This section contains important notes about IPSec CLI support on the Cisco ASR 1000 Series Router.

For information about Cisco IOS IPSec commands, see Cisco IOS Security Command Reference at the following location:


- The show crypto engine command, which displays information about the crypto engine, is not currently supported on the Cisco ASR 1000 Series Router. The unsupported show crypto engine subcommands include the following:
  - accelerator (Shows crypto accelerator information.)
  - brief (Shows all crypto engines in the system.)
  - configuration (Shows crypto engine configuration.)
  - connections (Shows connection information.)
The Cisco ASR 1000 Series Router does not currently support the display of send and recv error statistics using the `show crypto ipsec sa identity` command.

The Cisco ASR 1000 Series Router does not support the `clear` and `show crypto` commands on the standby Route Processor (RP) by design.

Counters in the `show platform software ipsec fp active flow identifier n` command are flagged for reset on read. You can use the `show crypto ipsec sa` command to obtain integral counters.

The `show access-list` command output does not show a packet count matching the ACL.

The Cisco ASR 1000 Series Router displays debugging information about the consumption of IPsec datapath memory; use the `show platform hardware qfp act feature ipsec datapath memory` command in privileged EXEC or diagnostic mode.

The Cisco ASR 1000 Series Router displays debugging information about the crypto engine processor registers; use the `show platform software ipsec f0 encryption-processor registers` command in privileged EXEC or diagnostic mode.

**Crypto Map Support**

This section contains important notes about IPSec crypto map support on the Cisco ASR 1000 Series Router:

- The Cisco ASR 1000 Series Router does not currently support IPSec tunnel configuration for crypto maps with same IP address on both the tunnel interface and the physical interface. Configurations with different IP addresses are supported.

- A possible Embedded Services Processor (ESP) reload may occur if a large number (such as 2000) of crypto maps are removed simultaneously. When removing a large number of crypto maps, it is recommended you unconfigure 500 crypto maps at a time and wait 25 seconds between operations.

- The Cisco ASR 1000 Series Router does not support the `show access-lists id` command under crypto maps.

- The Cisco ASR 1000 Series Router does not currently support the `interface range` command when configuring crypto maps.

**IPSec Packet Processing**

This section contains important notes about IPSec packet processing on the Cisco ASR 1000 Series Router:

- Reloading an Embedded Services Processor (ESP) on the Cisco ASR 1000 Series Router may cause a few IPSec packets to drop before the initialization completes, but the traffic will resume after a brief interval.

- The Cisco ASR 1000 Series Router will not discard an incoming IP datagram containing a Payload Length other than 4 in the authentication header (AH). For example, a 96 bit authentication value plus the 3 32-bit word fixed portion for any non-null authentication algorithm will not be discarded.

- The Cisco ASR 1000 Series Router does not forward incoming authenticated packets with the IP option field set.

**GET VPN Support**

This section contains important notes about Group Encrypted Transport VPN (GET VPN) support on the Cisco ASR 1000 Series Router:

- To ensure normal traffic flow for a GET VPN configuration on a Cisco ASR 1000 Series Router, a Time Based Anti Replay (TBAR) window-size of greater than 42 seconds is recommended.
Important Notes

- The Cisco ASR 1000 Series Router does not currently support the TBAR statistics display in the `show crypto gdoi gm replay` command.
- The Cisco ASR 1000 Series Router does not currently support Easy VPN (EzVPN) and GET VPN on the same interface.
- When a Cisco ASR 1000 Series Router is to apply the same Group Domain of Interpretation (GDOI) crypto maps to two interfaces, you should use local addresses for the crypto maps. Non-local address configuration is not supported.
- The Cisco ASR 1000 Series Router does not currently support transport mode for TBAR.
- The Cisco ASR 1000 Series Router only supports the reassembly of post-fragmented GET VPN packets that are destined for the local Cisco ASR 1000 Series Router in the GET VPN network.
- An enhancement is added to enable reassembly of IPsec transit traffic. This enhancement applies only to post-encryption fragmented IPsec packets. When this enhancement is enabled, IPsec will detect transit IPsec traffic and reassemble it before decryption. GET VPN transit IPsec traffic will be reassembled, decrypted, and forwarded to the destination. Non GET VPN transit IPsec traffic will be reassembled but not decrypted (because the Cisco ASR 1000 router is not the IPsec tunnel end point) and then forwarded to the destination.

To enable IPsec reassembly of transit traffic, use the `platform ipsec reassembly transit` command in global configuration mode. To disable IPsec reassembly of transit traffic, use the `no` form of this command.

```
platform ipsec reassembly transit
[no] platform ipsec reassembly transit
```

IPSec SSO and ISSU Support Notes

- The Cisco ASR 1000 Series Router supports stateful IPsec sessions on ESP switchover. During ESP switchover, all IPsec sessions will stay up and no user intervention is needed to maintain IPsec sessions.
- For an ESP reload (no standby ESP), the SA sequence number restarts from 0. The peer router drops packets that do not have the expected sequence number. User may need to explicitly reestablish IPsec sessions to work around this issue for systems that have a single ESP after an ESP reload. User may experience traffic disruption over the IPsec sessions in such cases for the duration of the reload.
- The Cisco ASR 1000 Series Router currently does not support Stateful Switchover (SSO) IPsec sessions on Route Processors (RPs). The IPsec sessions will go down on initiation of the switchover, but will come back up when the new RP becomes active. No user intervention is needed. User will experience traffic disruption over the IPsec sessions for the duration of the switchover, until the sessions are back up.
- The Cisco ASR 1000 Series Router currently does not support stateful ISSU for IPsec sessions. Before performing an ISSU, users must explicitly terminate all existing IPsec sessions or tunnels prior to the operation and reestablish them post ISSU. Specifically, users must ensure that there are no half-open or established IPsec tunnels present before performing ISSU. To do this, we recommend user do a interface shutdown in the case of interfaces that may initiate a tunnel setup, such as a routing protocol initiating a tunnel setup, or interfaces that have keepalive enabled or where there is an auto trigger for an IPsec session. Traffic disruption over the IPsec sessions during ISSU is obvious in this case.

Summarizing Caveats

- ESP—Switchover (with standby ESP):Stateful:IPSec sessions should be up. No user intervention needed.
• ESP—Reload (no standby ESP): Stateless: IPSec sessions will go down and come back. Usually, no user intervention is needed. However, users may have to explicitly re-establish an IPSec session if antireplay is configured (sequence number checking).

• RP—Switchover (with standby RP): Stateless: IPSec sessions will go down on RP switchover and the session should re-establish automatically when the new RP gains an active role. No user intervention is needed.

• ISSU (irrespective of chassis type): Stateless: Users must explicitly terminate all the IPSec sessions by shutting the interfaces, perform ISSU, and then re-establish tunnels by enabling the interfaces. No other intervention is needed.

Miscellaneous IPSec Support Notes
This section contains miscellaneous important notes about IPSec support on the Cisco ASR 1000 Series Router:

• In the context of an IPSec DVTI connection, the Cisco ASR 1000 Router does not support dynamic download ACL rule (per-user attribute) from the AAA server.

For example, the following configurations are not supported:

cisco-avpair += "ip:inacl#1=permit ip any 2.2.2.0 0.0.0.255"
cisco-avpair += "ip:outacl#1=permit ip 2.2.2.0 0.0.0.255 any"

• The Cisco ASR 1000 Router does not support the command of “if-state nhrp” in configuring the tunnel.

• The Cisco ASR 1000 Router Dead Peer Detection behavior is different than the pre-defined behavior (i.e. when there is no traffic to be sent, no DPD is sent, while if any traffic to be sent, DPD is sent). A Cisco ASR 1000 Router DPD is sent out regardless there is outbound traffic needs to be sent out.

• The Cisco ASR 1000 Router does not support SA Path MTU on data path.

• The Cisco ASR 1000 Router does not support double ACL in dynamic crypto map.

• VRF without crypto map configured on a physical interface causes dual esp reload on a Cisco ASR 1000 Router.

• The command: show crypto ipsec sa identity does not log send and receive error counts.

• The commands: clear crypto and show crypto on Standby RP are inconsistent with Active RP. At present most of other features disable ‘clear commands’ from Standby RP, but IPSec still allows to clear sa, session etc. from the standby.

• The Cisco ASR 1000 Router does not support Cisco AAA av-pair “cisco-avpair += ip:sub-policy-In=policy1”.

• CLI allows both ikev1 and ikev2 profile configured under the same crypto map, even though it is not supported internally on the ASR 1000 Router.

• For a Cisco ASR 1000 Router, the tunnel protection should be removed first before changing any configuration for tunnel protection.

• The security association (SA) maximum transmission unit (MTU) calculation is based on the interface MTU instead of the IP MTU.

• The Cisco ASR 1000 Series Router currently supports a maximum anti-replay window value of 512. If you attempt to configure a value larger than 512, the Cisco ASR 1000 Series Router defaults back to 512 internally (although the display still shows your user-configured value).

• The Cisco ASR 1000 Series Router does not currently support nested SA transformation such as:

crypto ipsec transform-set transform-1 ah-sha-hmac esp-3des esp-md5-hmac
crypto ipsec transform-set transform-1 ah-md5-hmac esp-3des esp-md5-hmac
• The Cisco ASR 1000 Series Router does not currently support Cisco IOS Certificate Authority (CA) server features.

• The Cisco ASR 1000 Series Router does not currently support COMP-LZS configuration.

• On Cisco ASR 1000 Series Routers, when configuring GRE over IPSec, it is recommended that you use only the tunnel protection mode on the tunnel interface. Using crypto maps on both the tunnel interface and the physical interface to achieve GRE over IPSec is not the supported method of configuration.

• When using dynamic VTI-based IPSec on a Cisco ASR 1000 Router, if there are multiple remote IPSec endpoints behind the same NAT device, only one of the endpoints has connectivity. In other words, multiple endpoints cannot have connectivity at the same time.

NAT and Firewall ALG Support on the Cisco ASR 1000 Series Routers

NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers matrix summarizes Network Address Translation (NAT) and Firewall Application Layer Gateway (ALG) feature support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1.0 and later releases. The matrix lists feature support by release. NAT and Firewall ALG support is cumulative; features introduced in earlier releases continue to be supported in later releases. You can find the matrix at the following location:


Important Notes About Cisco IOS XE Release 3.3.1S

This section provides important notes about Cisco IOS XE Release 3.3.1S and later releases.

Broadband Encapsulation Autosense Support Notes

This section contains important notes about the support for broadband encapsulation autosense with RBE configuration in Cisco IOS XE Release 3.3.1S:

• The broadband encapsulation autosense enhancement enables broadband autosense support for PPPoEoA, PPPoA, and RBE.

• In the Cisco IOS XE releases prior to Release 3.3.1S, aal5autopp encapsulation was not supported when an RBE was configured. As a result, the combination of aal5autopp encapsulation with RBE was not supported in the Cisco IOS XE releases prior to Release 3.3.1S.

• The broadband encapsulation enhancement in Cisco IOS XE Release 3.3.1S supports the combination of aal5autopp encapsulation with RBE-related configurations.

Important Notes About Cisco IOS XE Release 3.3.0S

This section provides important notes about Cisco IOS XE Release 3.3.0S and later releases.

High Availability on SBC

The following is the expected behavior of a session border controller (SBC) on which the High Availability feature is configured:
If switchover occurs while an H.323–H.323 T.38 fax transmission is in progress, the call does not fall back to the voice mode after the completion of the fax transmission. This is because the signaling state is not preserved in the event of a switchover.

**IPsec Failover**

IPSec failover is a feature that increases the total uptime (or availability) of your IPSec network. Traditionally, this is accomplished by employing a redundant (standby) router in addition to the original (active) router. If the active router becomes unavailable for any reason, the standby router takes over the processing of IKE and IPSec.

IPSec failover falls into two categories: stateless failover and stateful failover. The IPSec on the Cisco ASR 1000 Series Router supports only stateless failover. Stateless failover uses protocols such as the Hot Standby Router Protocol (HSRP) to provide primary to secondary cutover and also allows the active and standby VPN gateways to share a common virtual IP address.

**Important Notes About Cisco IOS XE Release 3.2.1S**

This section describes important notes about Cisco IOS XE Release 3.2.1S and later releases.

**EzVPN Support on Cisco ASR 1000 Series Routers**

On a ASR Cisco 1000 Router, when an EzVPN session is ended, the EzVPN server sends out a Stop Accounting message. This message does not contain the Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, and Acct-Output-Packets fields. It might cause a disruption of accounting performed on traffic.

**Maximum IP MTU for Loopback Interfaces**

For loopback interfaces, the maximum IP MTU is now 4000. This is to match the serial interface limits.

**Important Notes About Cisco IOS XE Release 3.2.0S**

This section describes important notes about Cisco IOS XE Release 3.2.0S and later releases.

**Cisco ASR 1001-4XT3**

Cisco ASR1001-4XT3 chassis functionality is similar to the SPA-4XT3/E3 with the exception of E3 circuitry in Cisco IOS XE 3.2.0S Release.

**SIP Trunk Over TCP**

SIP TCP trunk calls may not activate if more than one complete SIP messages were contained in one TCP segment in Cisco IOS XE 3.2.0S Release.
This symptom occurs upon SIP trunk over TCP scenario. SIP ALG currently processes only one complete SIP message in one TCP segment (one complete or one complete plus one incomplete), refer to CSCti56370.

**TCP Failover in Hardware High-Availability Mode**

TCP failover is not supported in Hardware High-Availability mode. If the active node fails in Hardware High Availability mode and if the network is restored, it may take 5 to 10 minutes for the standby node to become the active node. This is because of the reboot and the peer negotiation delay. If the network is not restored, only the switched over active peer is available. Failover is not possible in this state.

**Extended ACL as a WCCP Redirect ACL**

The Cisco ASR 1000 Series Router supports the use of an extended ACL as a WCCP redirect ACL. However, the option to specify a port range is not supported.

**Important Notes About Cisco IOS XE Release 3.1.1S**

This section describes important notes about Cisco IOS XE Release 3.1.1S and later releases.

**SIP-40G:SPA-4XT-SERIAL**

Cisco SPA-4XT-SERIAL was not supported in 3.1.0S when plugged into an ASR1000 with SIP-40. This SPA is supported in Release 3.1.1S on SIP-40 linecard.

For more information, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation, see section for SPA-4XT-Serial SPA in Table 1-4 (SIP and SPA Compatibility for Serial SPAs).


Cisco ASR1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide


**Important Notes About Cisco IOS XE Release 3.1.0S**

This section describes important notes about Cisco IOS XE Release 3.1.0S and later releases.

**Bidirectional Forwarding Detection (BFD)**

In Cisco IOS XE Release 3.1.0S, Bidirectional Forwarding Detection (BFD) is no longer supported in IP Base software packages. For BFD support, use the Advanced IP Services or Advanced Enterprise Services packages.
DMVPN Spoke Support

In Cisco IOS XE Release 3.1.0S Cisco ASR 1000 Series Routers do not support the `ip nhrp server-only` command if they act as DMVPN spokes.

Important Notes About Cisco IOS XE Release 2.6.0

This section describes important notes about Cisco IOS XE Release 2.6.0 and later releases.

Per-User Attribute on PPP Virtual Access

In Cisco IOS XE Release 2.6.0 multiple instances of the per-user attribute ‘Cisco-Avpair=lcp:interface-config=<cmd>’ is not supported.

For example:
Cisco-AVPair = lcp:interface-config=ip vrf forwarding vpngreen
Cisco-AVPair= lcp:interface-config=ip unnumbered loopback2

Should be configured like this in Cisco IOS XE Release 2.6.0:
Cisco-AVPair = lcp:interface-config=ip vrf forwarding vpngreen 
\ ip unnumbered loopback2
“Multiple instances will be supported in Cisco IOS XE Release 2.6.1”

Legacy QoS Command Deprecation: Hidden Commands

To streamline Cisco IOS QoS (quality of service), certain commands are being hidden. Although these commands are available in Cisco IOS XE Release 2.6, the CLI interactive help does not display them. If you attempt to view a command by entering a question mark at the command line, the command does not appear. However, if you know the command syntax, you can enter it. The system will accept the command and return a message explaining that it will soon be removed. These commands will be completely removed in a future release, which means that you will need to use the appropriate replacement commands.

For more information, see the following document:

VRF-Aware NAT

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.5.0

This section describes important notes about Cisco IOS XE Release 2.5.0 and later releases.
Embedded Packet Capture

The Embedded Packet Capture (EPC) feature is not functional and not supported for the Cisco ASR 1000 Series Routers.

QoS: Policing Support for GRE Tunnels

When queuing feature on the GRE tunnel interface is not supported with crypto configured on the physical interface.

QoS: Support for GRE/sVTI Tunnel

With IOS XE 2.5.0, the Cisco ASR 1000 Router Series supports Quality-of Service (QoS) applied to

- A GRE or sVTI tunnel with policing and marking only for INGRESS traffic
- A GRE or sVTI tunnel with 2-level hierarchy allowing queuing on the second level for EGRESS traffic

When there are multiple egress physical interfaces for a tunnel, and the tunnel target physical interface changes as a result of tunnel target destination route change, either manually by user configuration or by routing protocol, IOS will not prevent the tunnel traffic from moving to an alternate egress physical interface. However, in IOS XE 2.5.0, QoS tunnel move feature is not supported. When tunnel traffic moved to an alternate egress physical interface, tunnel QoS policy may enter a suspended state. At this point, the tunnel QoS policy will have to be removed and reapplied to the tunnel interface for it to take effect. In addition, queuing features on the GRE tunnel interface are not supported when IPSec is configured on the physical interface.

VRF-Aware NAT

Integrating NAT with MPLS VPNs

This section provides information about integrating NAT with MPLS VPNs.

Prerequisites for Integrating NAT with MPLS VPNs

Before performing the tasks in this module, you should be familiar with the concepts related to configuring NAT for IP address conservation. All access lists required for use with the tasks in this module should be configured prior to beginning the configuration task. For information about how to configure an access list, see IP Access List Sequence Numbering at the following location:


Note If you specify an access list to use with a NAT command, NAT does not support the commonly used permit ip any command in the access list.

Restrictions for Integrating NAT with MPLS VPNs

- The following functionality is not supported for VRF-Aware NAT:
  - VPN to VPN translations. In other words, VRF cannot be applied on the NAT outside interface.
  - Translation of multicast packets
  - Translations with inside destinations
  - Reversible route maps
Important Notes About Cisco IOS XE Release 2.3.0

This section describes important notes about Cisco IOS XE Release 2.3.0 and later releases.

Any Transport Over MPLS (AToM) Support

The configuration of Any Transport Over MPLS (AToM) on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.3.0 is only supported on a subinterface; AToM cannot be configured on the main interface. In addition, you cannot have any IP configuration on the main interface when you have an AToM configuration on the subinterface. These configuration guidelines are applicable to VC mode, VP mode, and L2VPN PW redundancy.

MPLS TE Support

Cisco ASR 1000 Series Router users considering the implementation of MPLS TE are recommended to consult with their local Cisco technical support representative for Cisco IOS XE implementation details.

VRF-Aware NAT

Dependency of NAT on VFR

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.2.2

This section describes important notes about Cisco IOS XE Release 2.2.2 and later releases.

Important Notes

- MIBs
- MPLS traffic engineering

- Configuring inside dynamic translations defined with outside interface mappings is not supported.
- Configuring inside static translations with interface mappings is not supported. The following commands, which do not include VRF, are not supported:
  - `ip nat inside source static esp local-ip interface type number`
  - `ip nat inside source static local-ip global-ip route-map name`
  - `ip nat inside source static local-ip interface type number`
  - `ip nat inside source static tcp local-ip local-port interface type number global-port`
  - `ip nat inside source static udp local-ip local-port interface type number global-port`

Dependency of NAT on VFR

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.
**SSO for L2TP Tunnel Switching Not Supported**

If dual route processors (RPs) are used on the Cisco ASR 1000 Series Router in Cisco IOS XE Release 2.2.2 and L2TP Tunnel Switching is configured, then `no l2tp sso enable` must be configured.

**VRF-Aware NAT**

**Dependency of NAT on VFR**

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces and environments in Cisco IOS XE Release 2.2.2. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

**Important Notes About Cisco IOS XE Release 2.2.1**

This section describes important notes about Cisco IOS XE Release 2.2.1 and later releases.

**100M FX SFP Not Supported on Cisco 2-Port Gigabit Ethernet Shared Port Adapter**

The 100M FX SFP is not supported on the Cisco 2-Port Gigabit Ethernet Shared Port Adapter (2x1GE SPA) on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2.1.

**Intelligent Service Gateway (ISG) Features Not Supported**

The following Intelligent Service Gateway (ISG) features are not supported on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2.1:

- ISG IP subscriber functionality on the following types of access interfaces: Gigabit EtherChannel (GEC) (Port Channel), generic routing encapsulation (GRE), PPP (virtual-template), and Layer 2 Tunneling Protocol (L2TP)
- ISG prepaid billing
- ISG IP interface sessions
- Interface statistics for ISG multiservice interfaces
- Access lists cannot be configured as match criteria in ISG Layer 4 redirect configuration. As an alternative, Layer 4 redirect should be configured in ISG traffic class services.
- Stateful Switchover (SSO and in-service software upgrade (ISSU) for ISG IP subscriber sessions or traffic class sessions. Upon switchover, an IP session must be recreated or restarted (for Dynamic Host Configuration Protocol (DHCP) sessions) when the session becomes active again.
- SSO and ISSU for any features on IP subscriber sessions or traffic class sessions
- SSO and ISSU for the following features on ISG PPP sessions:
  - Port-Bundle Host Key
  - Layer 4 Redirect
  - Traffic Class
Per-Session Multicast Support

Enhancements to the IP multicast feature provide support for per-session multicast in broadband environments in Cisco IOS XE Release 2.2.1.

VRF-Aware NAT

Dependency of NAT on VFR

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces and environments in Cisco IOS XE Release 2.2.1. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.1.1

This section describes important notes about Cisco IOS XE Release 2.1.1 and later releases.

Startup Configuration File Backup

As a matter of routine maintenance on any Cisco router, users should backup the startup configuration file by copying the startup configuration file from NVRAM onto one of the router’s other file systems and, additionally, onto a network server. Backing up the startup configuration file provides an easy method of recovering the startup configuration file in the event the startup configuration file in NVRAM becomes unusable for any reason.

For users using any Cisco ASR 1000 Series Router with a single RP, including any Cisco ASR 1002 or Cisco ASR 1004 Router, backing up the startup configuration file onto another router file system is especially important due to CSCsq70140, which is documented in the Caveats section of these release notes. The workaround for users who run into this caveat is to replace the startup configuration file in NVRAM with a backup copy of the startup configuration file on the router; therefore, customers who have backed up their startup configuration files onto the router will be ready to resolve these caveats if they occur on their Cisco ASR 1000 Series Routers using a single RP.

Example 1: Copying Startup Configuration File to Bootflash

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 May 29 2008 16:31:41 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
12 -rw- 208904396 May 28 2008 16:17:34 -07:00 asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin

Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]?

3517 bytes copied in 0.647 secs (5436 bytes/sec)

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
Example 2: Copying Startup Configuration File to USB Flash Disk

Router# dir usb0:
Directory of usb0:/

43261 -rwx 208904396 May 27 2008 14:10:20 -07:00
asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin

255497216 bytes total (40190464 bytes free)

Router# copy nvram:startup-config usb0:
Destination filename [startup-config]?

3172 bytes copied in 0.214 secs (14822 bytes/sec)

Router# dir usb0:
Directory of usb0:/

43261 -rwx 208904396 May 27 2008 14:10:20 -07:00
asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin
43262 -rwx 3172 Jul 2 2008 15:40:45 -07:00 startup-config

255497216 bytes total (40186880 bytes free)

Example 3: Copying Startup Configuration File to a TFTP Server

Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.17.16.81
Destination filename [pe24_asr-1002-config]? /auto/tftp-users/user/startup-config
!!

3517 bytes copied in 0.122 secs (28828 bytes/sec)

VRF-Aware NAT

Dependency of NAT on VFR
ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.1.0

This section describes important notes about Cisco IOS XE Release 2.1.0 and later releases.

High-Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers

Table 1 describes some of the high level feature sets that are not supported for the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1.0 and later releases. Use Cisco Feature Navigator to confirm support for a specific feature. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Feature support is subject to change from release to release. Some high-level feature sets that were not supported in the initial Cisco IOS XE Release 2.1.0 are now supported. Table 1 has been updated to indicate when support has been introduced in later releases. For the latest feature information, see the New and Changed Information sections of these release notes and Cisco Feature Navigator.

Table 1  High-Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers

<table>
<thead>
<tr>
<th>Major Feature Category</th>
<th>Features Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>Support for ATM features begins in Cisco IOS XE Release 2.3.0. No ATM features are supported in earlier releases.</td>
</tr>
<tr>
<td>Broadband</td>
<td>Support for ANCP begins in Cisco IOS XE Release 2.4.0. ANCP is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>IPv6 Intelligent Service Gateway (IPv6 ISG)</td>
</tr>
<tr>
<td></td>
<td>MLP over ATM (MLPoATM)</td>
</tr>
<tr>
<td></td>
<td>MLP over Ethernet (MLPoE)</td>
</tr>
<tr>
<td></td>
<td>Multilink PPP on L2TP Network Server (MLPPP on LNS)</td>
</tr>
<tr>
<td></td>
<td>Point-to-Point Protocol over Ethernet Tag (PPPoE Tag)</td>
</tr>
<tr>
<td></td>
<td>PPP over Q-in-Q (PPPoQinQ)</td>
</tr>
<tr>
<td>Ethernet OAM</td>
<td>Ethernet Operation, Administration, and Maintenance (OAM)</td>
</tr>
<tr>
<td>MPLS</td>
<td>Support for Carrier’s Carrier begins in Cisco IOS XE Release 2.2.3. Carrier’s Carrier is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>Support for Ethernet over MPLS (EoMPLS) begins in Cisco IOS XE Release 2.4.0. Ethernet over MPLS (EoMPLS) is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>Support for Inter-AS begins in Cisco IOS XE Release 2.2.2. Inter-AS is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>IPv6 Provider Edge Router over MPLS (6PE)</td>
</tr>
<tr>
<td></td>
<td>IPv6 VPN over MPLS (6VPE)</td>
</tr>
<tr>
<td></td>
<td>Label Distribution Protocol (LDP) Session Protection</td>
</tr>
<tr>
<td></td>
<td>Support for Layer 2 VPN (L2VPN) begins in Cisco IOS XE Release 2.3.0. L2VPN is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>Support for MPLS Traffic Engineering/Fast Reroute (MPLS TE/FRR) begins in Cisco IOS XE Release 2.3.0. MPLS TE/FRR is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>Virtual Private LAN Service (VPLS)</td>
</tr>
<tr>
<td>Multicast</td>
<td>Multicast VPN</td>
</tr>
<tr>
<td>Routing</td>
<td>Performance Routing/Optimized Edge Routing (PFR/OER)</td>
</tr>
</tbody>
</table>
### Important Notes

**Security**
- Support for Group Encrypted Transport VPN (GET VPN) begins in Cisco IOS XE Release 2.3.0. GET VPN is not supported in earlier releases.
- IPv6 IPSec
  - Support for Lawful Intercept begins in Cisco IOS XE Release 2.4.0. Lawful Intercept is not supported in earlier releases.
- VRF-Aware Firewall
  - Support for VRF-Aware NAT when running ASRNAT this will not handle fragmented packets unless VFR is configured on all NAT interfaces.

**Voice**
- Support for Cisco Unified Border Element (SP Edition) begins in Cisco IOS XE Release 2.4.0. Cisco Unified Border Element (SP Edition) is not supported in earlier releases. Earlier releases include support for Integrated Session Border Controller.

---

**Table 1**  
*High-Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers (continued)*

<table>
<thead>
<tr>
<th>Major Feature Category</th>
<th>Features Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Support for Group Encrypted Transport VPN (GET VPN) begins in Cisco IOS XE Release 2.3.0. GET VPN is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>IPv6 IPSec</td>
</tr>
<tr>
<td></td>
<td>Support for Lawful Intercept begins in Cisco IOS XE Release 2.4.0. Lawful Intercept is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>VRF-Aware Firewall</td>
</tr>
<tr>
<td></td>
<td>Support for VRF-Aware NAT when running ASRNAT this will not handle fragmented packets unless VFR is configured on all NAT interfaces.</td>
</tr>
<tr>
<td>Voice</td>
<td>Support for Cisco Unified Border Element (SP Edition) begins in Cisco IOS XE Release 2.4.0. Cisco Unified Border Element (SP Edition) is not supported in earlier releases. Earlier releases include support for Integrated Session Border Controller.</td>
</tr>
</tbody>
</table>
New Features in and Important Notes About Cisco IOS XE 3.2S Releases

This chapter provides information about the new features introduced in the Cisco IOS XE 3.2S releases. In addition, important notes about these releases are included in this chapter.

Cisco IOS XE 3S releases inherit all Cisco IOS XE Release 2 features that were released prior to the introduction of the Cisco IOS XE 3S releases with few exceptions. For information about inherited features that were introduced in Cisco IOS XE Release 2 releases, for a list of new and changed features, and important notes that apply to Cisco IOS XE Release 2, see the “New and Changed Information” section in Cisco IOS XE Release 2 Release Notes.

This chapter contains the following sections:

- New and Changed Information, page 143
- Important Notes, page 159

New and Changed Information

This section lists the new hardware and software features that are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.2S and contains the following sections:

- New Hardware Features in Cisco IOS XE Release 3.2.2S, page 143
- New Software Features in Cisco IOS XE Release 3.2.2S, page 144
- New Hardware Features in Cisco IOS XE Release 3.2.1S, page 144
- New Software Features in Cisco IOS XE Release 3.2.1S, page 144
- New Hardware Features in Cisco IOS XE Release 3.2.0S, page 144
- New Software Features in Cisco IOS XE Release 3.2.0S, page 146

New Hardware Features in Cisco IOS XE Release 3.2.2S

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.2.2S.
New Software Features in Cisco IOS XE Release 3.2.2S

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.2.2S.

New Hardware Features in Cisco IOS XE Release 3.2.1S

There are no new hardware features in the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.2.1S.

New Software Features in Cisco IOS XE Release 3.2.1S

The following are the new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.2.1S:

SSO/ISSU Support for Per-User IPv6 ACL for PPP Sessions

The SSO/ISSU Support for Per-User IPv6 ACL for PPP Sessions feature reproduces the IPv6 ACLs that are present on the active RP to the standby RP, and provides a consistent SSO and ISSU experience for active sessions. This feature also extends the ability to maintain Template ACLs (IPv6 only or dual stack) through ISSU and SSO.

For more information, see Implementing Traffic Filters and Firewalls for IPv6 Security at the following location:

Frame Relay over MPLS

Frame Relay over MPLS encapsulates Frame Relay PDUs in MPLS packets and forwards them across the MPLS network. For Frame Relay, you can set up DLCI-to-DLCI connections or port-to-port connections.

For more information, see Any Transport over MPLS at the following location:

New Hardware Features in Cisco IOS XE Release 3.2.0S

The following new hardware features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.2.0S:

Cisco ASR 1001 Router

Cisco ASR 1001 Router is a small form factor router targeted for high-end branch offices needing integrated services including voice and security with high-speed connectivity (2.5Gbps w/optional SW license for 5 Gbps). Designed with integrated Cisco ASR1000-RP, Cisco ASR1000-SIP, Cisco
New Features in and Important Notes About Cisco IOS XE 3.2S Releases

ASR1000-ESP with Nitrox running IOS-XE software RLS 3.2S. Input/output options include a half-height SPA, 4x1GE built-in ports, and a factory-installed integrated daughter card (IDC) with different options.

For more information, see the following documents:

Cisco ASR 1000 Series Aggregation Services Router Hardware Installation Guide

Quick Start Guide for the Cisco ASR 1001 Router

Cisco ASR 1000-ESP40 and Cisco ASR 1000-SIP40 on the Cisco ASR 1004 Router

To meet requirements from customers who have already installed the Cisco ASR 1004 Router and have limited rack space and require higher bandwidth, the Cisco ASR 1000-ESP40 and the Cisco ASR 1000-SIP40 are now supported on the Cisco ASR 1004 Router in Cisco IOS XE 3.20S Software Release.

For more information, see the following documents:

Cisco ASR 1000 Series Aggregation Services Router Hardware Installation Guide

Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide

Cisco Synchronization Service SPA

Cisco Synchronization Service SPA is a 2 x1 GE SPA with specialized synchronization services function built in to provide Synchronization over packet networks including support for BITS, SyncE, SSM, 1588-2008, GPS receiver and timing interfaces.

For more information, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide

Cisco DSP SPA

The Cisco DSP SPA for Cisco ASR 1000 Series Routers is a half-height SPA that provides voice transcoding and transrating functionalities for media streams using different codecs.

For more information, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide
New Software Features in Cisco IOS XE Release 3.2.0S

The following new software features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.2.0S. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes.

ANCP Values Configuration Support on LNS

This feature will allow for two functionalities when the BRAS enables the tx/rx speed values for a subscriber, without the CLI:

1. From RADIUS (configured in profile)
2. From ANCP sent by DSLAM.

This new functionality provides away in configuring RX/TX connection speeds for both instances.

For more information, see Configuring AAA for VPDNs at the following location:

ANCP—CLI Technology Improvements

To improve ANCP troubleshooting, the following commands were introduced or modified in Cisco IOS XE Release 3.2S:

- debug ancp: Enables the display of debugging information related to Access Node Control Protocol (ANCP).
- how ancp an-port: Displays information about ANCP Access Node (AN) ports.
- how ancp an-port circuit-id: Displays information about an ANCP AN port and the corresponding subscriber access line identified by the subscriber circuit ID.
- how ancp an-port neighbor description: Displays information about the AN ports associated with an ANCP neighbor identified by a description name.
- how ancp an-port neighbor: Displays statistics of ANCP neighbor information and neighborship information with local ANCP ports.
- how ancp neighbor description: Displays brief information about an ANCP neighbor that is identified by a description name.
- how ancp neighbor sender-name: Displays brief information about an ANCP session that has a neighbor identified by an ANCP sender name.
- how ancp neighbor statistics: Displays message statistics of all active or configured ANCP neighbors.
- how ancp neighbor summary: Displays a summary of the ANCP neighbors.

For more information about these commands, see the following document:
New and Changed Information

Any Transport over MPLS (AToM)—ATM AAL5 over MPLS (AAL5oMPLS)

The AAL5 Transport over MPLS feature provides an ATM permanent virtual circuit (PVC) transport service for transporting AAL5 PDUs across an IP/MPLS backbone with rate-limit policing and configurable PVC priority value. A dynamic MPLS tunnel is configured to enable label imposition and disposition of encapsulated ATM PDUs transported between two edge routers having a Label Distribution Protocol (LDP) neighbor relationship.

For more information, see the following document:

Any Transport over MPLS (AToM)—ATM OAM Emulation

This feature allows for Any Transport over MPLS (AToM): ATM OAM Emulation support.

For more information, see the following document:

Any Transport over MPLS (AToM)—HDLC over MPLS (HDLCoMPLS)

This feature allows for transport HDLC packets across an MPLS backbone.

For more information, see the following document:

Any Transport over MPLS (AToM)—PPP over MPLS (PPPoMPLS)

This feature allows for transport PPP protocol data units (PDUs) across an MPLS backbone.

For more information, see the following document:

Application Inspection and Control for SMTP

The Application Inspection for SMTP feature provides an intense provisioning mechanism that can be configured to inspect packets on a granular level so that malicious network activity, related to the transfer of e-mail at the application level, can be identified and controlled. This feature qualifies the Cisco IOS firewall extended Simple Mail Transfer Protocol (ESMTP) module as an “SMTP application firewall,” which protects in a similar way to that of an HTTP application firewall.

For more information, see the following document:

ATM Routed Bridge Encapsulation (RBE)

The feature allows the router to receive RFC 1483 Ethernet frames on ATM interfaces that are routed on the Layer 3 header.

For more information, see the following document:
New Features in and Important Notes About Cisco IOS XE 3.2S Releases

BD (Bridge Domain) Infrastructure

BD (Bridge Domain) Infrastructure feature allows for enabling bridging functionality on the Cisco ASR 1000 Router Series.

For more information, see the following document:

BDI (Bridge Domain Interface)

The BDI (Bridge Domain Interface) feature provides Layer 3 termination for the bridge domain.

For more information, see the following document:

BGP—RT-Constrained Route Distribution

This feature automates RT Filter implementation of RT-Constraint. For more information, see the following document:

Cisco IOS Software Activation

Cisco Software Activation is a simplified approach to software deployment and management on the Cisco ASR 1000 Router Series.

This new infrastructure helps enable the following:
- Speed deployment and roll out new Cisco Software Activation feature sets across global networks
- Centrally and more accurately manage and track software and license compliance
- Easily conduct software compliance audits to meet regulations without impacting network operations

For more information, see the following document:

Cisco Unified Border Element (Enterprise)

The following Cisco Unified Border Element (Enterprise) features were introduced in Cisco IOS XE Release 3.2.0S:
- Box to Box (Interchassis) Redundancy
- RTP Port Range Configurable per Interface
- Stateful Switchover Between Redundancy Paired Intra or Inter-Box Devices

In addition, Cisco IOS XE Release 3.2.0S introduces support for Cisco Unified Border Element (Enterprise) DSP SPA:
- Support for DSP-based functionality on CUBE (ENT) including Transcoding and Transrating

For information about these Cisco Unified Border Element (Enterprise) features, see the following documents:
Cisco Unified Border Element (Enterprise) Configuration Guide
Cisco Unified Border Element (Enterprise) Configuration Guide: SIP Trunking for PSTN Access:
Cisco Unified Border Element (Enterprise) Configuration Guide: SIP-to-SIP Connections on a Cisco Unified Border Element:

**Cisco Unified Border Element (SP Edition)—Unified Model**

The following Cisco Unified Border Element (SP Edition) features were introduced in Cisco IOS XE Release 3.2.0S:
- Support on new ASR 1001 Chassis for Cisco Unified Border Element
- Analysis, Routing, and Policy Enhancements
- Billing: XML based billing
- Emergency and Security Enhancements
- Interchassis High Availability
- Media: Media Interworking Enhancements

In addition, Cisco IOS XE Release 3.2.0S introduces support for Cisco Unified Border Element (SP Edition) DSP SPA:
- Media:Transcoding:SBC Support For On-board DSP Services
- Media:DTMF Interworking:InBand and RFC2833/OOB (SIP INFO/NOTIFY)
- Media:DTMF Interworking:RFC2833 and OOB (SIP INFO/NOTIFY) for Calls Transcoded with Onboard DSPs
- Media:Transcoding:SIP to SIP Voice Transcoding support
- Media:Transcoding:Voice Transcoding Statistics and Error handling for SIP-SIP Calls
- Media:Voice Transrating Support
- SIP-SIP Call Capacity for DTMF Interworking between Inband and RFC2833
- SIP-SIP Call Capacity for Transcoding and Transrating Capabilities
- Support for DSP Based functionality including Transcoding and Transrating

For information about these Cisco Unified Border Element (SP Edition) features, see the following documents:


*Cisco Unified Border Element (SP Edition) Command Reference: Unified Model*

For information about these Cisco Unified Border Element (SP Edition) Distributed Model features, see the following documents:
Cisco Unified Border Element (SP Edition) Configuration Guide: Distributed Model

Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model

**Cisco Unified Border Element (SP Edition)—Distributed Model**

In addition, Cisco IOS XE Release 3.2.0S introduces support for Cisco Unified Border Element (SP Edition) DSP SPA:

- Media:Transcoding: SBC Support For On-board DSP Services
- Media:DTMF Interworking:InBand and RFC2833/OOB
- Media:DTMF Interworking:RFC2833 and OOB for Calls Transcoded with Onboard DSPs
- Media:Voice Transrating support
- Support for DSP Based functionality including Transcoding and Transrating

For information about these Cisco Unified Border Element (SP Edition) features, see the following documents:


For information about these Cisco Unified Border Element (SP Edition) Distributed Model features, see the following documents:

Cisco Unified Border Element (SP Edition) Configuration Guide: Distributed Model

Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model

**DHCP Lease Limit Per ATM/RBE Unnumbered Interface**

This feature allows for DHCP Server and DHCP Relay Enhancements to limit the number of leases per ATM/RBE unnumbered interface.

For more information, see the following document:

**DHCPv6 Bulk Lease Query**

This feature provides support for RFC 5460 - DHCPv6 Bulk Lease query.

For more information, see the following document:
Easy Virtual Network EIGRP

For more information, see the following documents:


Easy Virtual Network MIB and Context-based SNMP Simplification

This feature allows for VNET MIB Support Autoconfiguration Context Aware VRF-aware for config copy MIB.

For more information, see the following document:


Easy Virtual Network OSPF

For more information, see the following documents:


EIGRP IPv6 VRF-Lite

For more information, see the following documents:


Enhanced NBAR

Cisco IOS XE 3.2S Release includes support for 32 new and 7 updated protocols.

For the complete list of supported and updated protocols, refer to the following document:


EVC Infrastructure

The Cisco ASR 1000 Router EVC infrastructure provides the capability for the Cisco ASR 1000 to classify Layer 2 traffic to various Ethernet Service Instances (EFP) on a physical port. Subsequently these EFP can be mapped to an EVC based forwarding services to accomplish Layer 2 forwarding.

For more information, see the following document:


Firewall ALG—SIP REFER Method

The Firewall ALG - SIP REFER Method feature is used for call transfers. A REFER message is used to refer to a peer. The REFER method indicates that the recipient of a call, identified by a request Uniform Resource Identifier (URI) must contact a third party using the contact information provided in the request.
The Firewall ALG - SIP REFER Method feature supports two types of call transfers, unattended (blind) transfer and attended (consultative) transfer. For more information on call flows, see the SIP Call Flows document.

**Firewall ALG—SIP Trunking Support**

A SIP trunk is a direct connection of an IP PBX to a service provider over an IP network using SIP. There can be numerous concurrent calls in a SIP trunk. During the call setup process, all these calls use the same control channel for call establishment. More than one call uses the same control channel for call setup. Using the same control channel by more than one call confuses the stateful information stored in the control channel session. The SIP stateful information consists of the media channel information such as IP address and port number used by client/server endpoints to send media data. The media channel information is used to create a door for the data channel in the firewall. Because multiple calls use the same control channel for call setup, there will be multiple sets of media data. The Firewall ALG-SIP Trunking Support feature uses a local database to store all the media-related information within a SIP trunk. Call IDs of each call are used to index this local database.

TCP segmentation in a SIP trunk can cause unexpected behavior that includes packet drops, TCP reset, and slow response.

**Flexible NetFlow—32-Bit AS Number Support**

This feature will allow for IOS-BGP that extends all ASN value from ushort to ulong for RFC 4893. BGP fields are defined in NetFlow and should be extended accordingly.

**Hierarchical Color-Aware Policing**

The Hierarchical Color-Aware Policing feature provides two levels of policing where the policer ordering is evaluated from child to parent, and there is preferential treatment of certain traffic at the parent level.

Beginning in Cisco IOS XE Release 3.2S, this feature is enabled on the Cisco ASR 1000 series Aggregation Services Routers through the following support and changes:

- Reverse the order of dataplane policing in hierarchical policies so that they are evaluated from child to parent. In prior releases, the policies are evaluated from parent to child.
- Limited support for color-aware policing (RFC 2697 and RFC 2698) within Quality of Service (QoS) policies.

For more information, see the following document:


**IEEE 802.1ag-2007 Compliant CFM**

The feature allows IEEE 802.1ag (Draft 8.1) Compliant CFM (Bridge Domain Support) support on the Cisco ASR 1000 Router Series.

For more information, see the following document:

Inbound Policy Marking for dVTI

This feature provides marking on a dVTI (no policing, or queuing features are supported.) Scale: 1000 dVTIs with a flat marking policy.

For more information, see the following document:

Ingress Packet Scheduling (Intra-CC and Inter-CC Ingress Scheduling)

Ingress packet scheduling is applicable to packets entering the Cisco ASR 1000 Router through an interface.

For more information, see the following document:

IP Routing of RFC1483 ATM Bridge Encapsulation (RBE)

For more information, see the following document:

IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731)

For more information, see the following document:

IPv6 ACL—Template ACL

The IPV6 Template ACL feature enables you to significantly scale the number of per-user access lists within a router

For more information, see the following document:

IPv6 Policy-Based Routing

For more information, see the following document:

ISSU—MPLS VPN 6VPE & 6PE ISSU Support

For more information, see the following document:
ISSU—RBE

For more information, see the following document:

Legacy QoS Command Deprecation—Removed Commands

This feature enables the qos legacy cli commands to be deprecated and replaced.
For more information, see the following document:

MoFRR (Multicast Only Fast Reroute)

For more information, see the following document:

MQC Hierarchical Classmap

Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) allows multiple traffic classes (nested traffic classes, which are also called nested class maps or MQC hierarchical class maps) to be configured as a single traffic class.
For more information, see the following document:

Multicast Live-Live

The Multicast Live-Live feature delivers two multicast streams with the same content over diverse paths in the network. This functionality reduces packet loss due to network failures on any one of the paths.
For more information, see the following document:

Multi-SA for DVTI

This feature enables DVTI to support multiple IPsec security associations.
For more information, see the following document:

MVPN—Data MDT Enhancements

Multicast distribution tree (MDT) groups were selected at random when the traffic passed the threshold and there was a limit of 255 MDTs before they were reused. The MVPN-Data MDT Enhancements feature provides the ability to deterministically map the groups from inside the VPN routing and forwarding (S,G) entry to particular data MDT groups, through an access control list (ACL).
The user can now map a set of VPN routing and forwarding (S,G) to a data MDT group in one of the following ways:

- 1:1 mapping (1 permit in ACL)
- Many to 1 mapping (many permits in ACL)
- Many to many mapping (multiple permits in ACL and a nonzero mask data MDT)

Because the total number of configurable data MDTs is 1024, the user can use this maximum number of mappings in any of the described combinations.

**NAT ALG—SIP REFER Method**

For more information, see the following document:

**NAT ALG—SIP Trunking Support**

For more information, see the following document:

**New DSP SPA Software Features**

The following new DSP SPA software features have been introduced in this release:

- Ability to disable comfort noise generation on system-wide basis
- Ability to Support Multiple Applications
- Ability to Translate Between Any Two Codec Types
- Comfort Noise Generation
- DSP Management (MIBs, Show Commands)
- Dynamic Jitter Buffer for Packet Loss Concealment
- Failed DSP Out of Allocation
- Multiple DSP Pools from Same DSP SPA
- Multiple Voice Codecs supported by DSPs
- OIR Support
- Pools of Multiple DSP SPAs
- Restart Failed DSP within 1sec
- Shared DSP Technology with IOS Voice Gateways
- Support VoIP/Video over IPv4 as well as IPv6
- Voice/Network Quality Stats Per Call Leg

For more information about Cisco ASR 1000 Series router support for the DSP SPA features, see:
Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide

For more information about the DSP SPA features, see:
Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide

**OSPF—Demand Circuit Disable**

For more information, see the following document:

**PKI High Availability**

For more information, see the following document:

**Policy Accounting Phase 2**

For more information, see the following document:

**Port Level Shaping Concurrent with 4HQoS on ES+**

For more information, see the following document:

**PPP IP Unique Address/Prefix Detection**

For more information, see the following document:

**PPP—IPv6 Accounting Delay Enhancements**

For more information, see the following document:

**QoS—Time-Based Thresholds for WRED and Queue Limit**

This feature introduces support for QoS over a GRE/sVTI VRF tunnels.
For more information, see the following document:
RADIUS Over IPv6

This feature allows for time-based thresholds for WRED and queue limit.
For more information, see the following document:

RADIUS Statistics VIA SNMP

This feature will enable RADIUS to work over IPv6 transport.
For more information, see the following document:

RSVP-VRF Lite Admission Control

This feature allows for RSVP CAC for IP-sessions within the context of a VRF.
For more information, see the following document: URL:

SNMP Enhancements for Cisco ASR 1000 Router

For more information, see the following document:

SSHv2 Enhancements for RSA Keys

This feature adds support for the following functionalities:
- RSA keys based user authentication for SSH
- SSH server host key storage and verification.
For more information, see the following document:

SSO—MPLS VPN 6VPE and 6PE SSO Support

For more information, see the following document:

SSO—RBE

For more information, see the following document:
Stateless Network Address Translation 64

For more information, see the following document:

Synchronous Ethernet (SyncE): ESMC and SSM

Supports Ethernet Synchronization Message Channel (ESMC) and the Synchronization Status Message (SSM) control protocol for SyncE to synchronize clock frequency over an Ethernet port with quality level selection.

For more information, see the following document:

Synchronous Ethernet Support

Synchronous Ethernet support is paramount for delivering timing information efficiently to the cellsite base stations. From Service Provider perspective, this solution overcomes the need to provide a separate TDM circuit for providing timing. SyncE will be as per ITU-T standards as defined in below mentioned Functional specifications. It will leverage physical layer of ethernet to transmit frequency to remote site.

For more information, see the following document:

Tacacs over IPv6

This feature will enable TACACS+ to work over IPv6 Transport.

For more information, see the following document:

VASI (VRF-Aware Software Infrastructure) Enhancements Phase II

This feature enhancement allows for VASI: VASI Enhancements with IPv6 unicast traffic and IPv4 dynamic routing protocols support (OSPF and EIGRP) support.

For more information, see the following document:

VFR Enhancements

For more information, see the following document:

Virtual Network Trunk

For more information, see the following documents:
VRF-Aware IPsec Phase III Support

For more information, see the following document:


VRF Route Replication

For more information, see the following document:


VRF-Aware Traceroute with VRF Name

For more information, see the following document:


Important Notes

The following sections contain important notes about Cisco IOS XE 3S Releases and later running on Cisco ASR 1000 Series Routers.

Deferrals

Cisco IOS software images are subject to deferral. We recommend that you view the deferral notices at the following location to determine whether your software release is affected:


Field Notices and Bulletins

- **Field Notices**—We recommend that you view the field notices for this release to determine whether your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

Important Notes About IPSec Support on the Cisco ASR 1000 Series Router

This section contains important notes about IPSec support on the Cisco ASR 1000 Series Router.

IPSec CLI Support Notes
This section contains important notes about IPSec CLI support on the Cisco ASR 1000 Series Router:


- The `show crypto engine` command, which displays information about the crypto engine, is not currently supported on the Cisco ASR 1000 Series Router. The unsupported `show crypto engine` subcommands include the following:
  - `accelerator` (Shows crypto accelerator information.)
  - `brief` (Shows all crypto engines in the system.)
  - `configuration` (Shows crypto engine configuration.)
  - `connections` (Shows connection information.)
  - `qos` (Shows QoS information.)

- The Cisco ASR 1000 Series Router does not currently support the display of send and recv error statistics using the `show crypto ipsec sa identity` command.

- The Cisco ASR 1000 Series Router does not support the `clear` and `show crypto` commands on the standby Route Processor (RP) by design.

- Counters in the `show platform software ipsec fp active flow identifier n` command are flagged for reset on read. You can use the `show crypto ipsec sa` command to obtain integral counters.

- The `show access-list` command output does not show a packet count matching the ACL.

- The Cisco ASR 1000 Series Router displays debugging information about the consumption of IPsec datapath memory; use the `show platform hardware qfp act feature ipsec datapath memory` command in privileged EXEC or diagnostic mode.

- The Cisco ASR 1000 Series Router displays debugging information about the crypto engine processor registers; use the `show platform software ipsec f0 encryption-processor registers` command in privileged EXEC or diagnostic mode.

Crypto Map Support
This section contains important notes about IPSec crypto map support on the Cisco ASR 1000 Series Router:

- The Cisco ASR 1000 Series Router does not currently support IPSec tunnel configuration for crypto maps with same IP address on both the tunnel interface and the physical interface. Configurations with different IP addresses are supported.

- A possible Embedded Services Processor (ESP) reload may occur if a large number (such as 2000) of crypto maps are removed simultaneously. When removing a large number of crypto maps, it is recommended you unconfigure 500 crypto maps at a time and wait 25 seconds between operations.

- The Cisco ASR 1000 Series Router does not support the `show access-lists id` command under crypto maps.

- The Cisco ASR 1000 Series Router does not currently support the `interface range` command when configuring crypto maps.
**IPSec Packet Processing**

This section contains important notes about IPSec packet processing on the Cisco ASR 1000 Series Router:

- Reloading an Embedded Services Processor (ESP) on the Cisco ASR 1000 Series Router may cause a few IPSec packets to drop before the initialization completes, but the traffic will resume after a brief interval.
- The Cisco ASR 1000 Series Router will not discard an incoming IP datagram containing a Payload Length other than 4 in the authentication header (AH). For example, a 96 bit authentication value plus the 3 32-bit word fixed portion for any non-null authentication algorithm will not be discarded.
- The Cisco ASR 1000 Series Router does not forward incoming authenticated packets with the IP option field set.

**GET VPN Support**

This section contains important notes about Group Encrypted Transport VPN (GET VPN) support on the Cisco ASR 1000 Series Router:

- To ensure normal traffic flow for a GET VPN configuration on a Cisco ASR 1000 Series Router, a Time Based Anti Replay (TBAR) window-size of greater than 42 seconds is recommended.
- The Cisco ASR 1000 Series Router does not currently support the TBAR statistics display in the `show crypto gdoi gm replay` command.
- The Cisco ASR 1000 Series Router does not currently support Easy VPN (EzVPN) and GET VPN on the same interface.
- When a Cisco ASR 1000 Series Router is to apply the same Group Domain of Interpretation (GDOI) crypto maps to two interfaces, you should use local addresses for the crypto maps. Non-local address configuration is not supported.
- The Cisco ASR 1000 Series Router does not currently support transport mode for TBAR.
- The Cisco ASR 1000 Series Router only supports the reassembly of post-fragmented GET VPN packets that are destined for the local Cisco ASR 1000 Series Router in the GET VPN network.
- An enhancement is added to enable reassembly of IPsec transit traffic. This enhancement applies only to post-encryption fragmented IPsec packets. When this enhancement is enabled, IPsec will detect transit IPsec traffic and reassemble it before decryption. GET VPN transit IPsec traffic will be reassembled, decrypted, and forwarded to the destination. Non GET VPN transit IPsec traffic will be reassembled but not decrypted (because the Cisco ASR 1000 router is not the IPsec tunnel end point) and then forwarded to the destination.

To enable IPsec reassembly of transit traffic, use the `platform ipsec reassembly transit` command in global configuration mode. To disable IPsec reassembly of transit traffic, use the no form of this command.

```
platform ipsec reassembly transit
genplatform ipsec reassembly transit
```

**IPSec SSO and ISSU Support Notes**

- The Cisco ASR 1000 Series Router supports stateful IPSec sessions on ESP switchover. During ESP switchover, all IPSec sessions will stay up and no user intervention is needed to maintain IPSec sessions.
For an ESP reload (no standby ESP), the SA sequence number restarts from 0. The peer router drops packets that do not have the expected sequence number. User may need to explicitly reestablish IPSec sessions to work around this issue for systems that have a single ESP after an ESP reload. User may experience traffic disruption over the IPSec sessions in such cases for the duration of the reload.

The Cisco ASR 1000 Series Router currently does not support Stateful Switchover (SSO) IPSec sessions on Route Processors (RPs). The IPSec sessions will go down on initiation of the switchover, but will come back up when the new RP becomes active. No user intervention is needed. User will experience traffic disruption over the IPSec sessions for the duration of the switchover, until the sessions are back up.

The Cisco ASR 1000 Series Router currently does not support stateful ISSU for IPSec sessions. Before performing an ISSU, users must explicitly terminate all existing IPSec sessions or tunnels prior to the operation and reestablish them post ISSU. Specifically, users must ensure that there are no half-open or established IPSec tunnels present before performing ISSU. To do this, we recommend user do a interface shutdown in the case of interfaces that may initiate a tunnel setup, such as a routing protocol initiating a tunnel setup, or interfaces that have keepalive enabled or where there is an auto trigger for an IPSec session. Traffic disruption over the IPSec sessions during ISSU is obvious in this case.

Summarizing and restating the different caveats:
- ESP - switchover (with standby ESP) : Stateful :
  - IPSec sessions should be up. No user intervention needed.
- ESP - Reload (No standby ESP) : Stateless :
  - IPSec sessions will go down and come back up. Usually no user intervention is needed. However, user may need to explicitly reestablish Ipsec session again if anti replay is configured (sequence number checking).
- RP - switchover (with standby RP) : Stateless :
  - IPSec sessions will go down on RP switchover and should reestablish themselves when the new RP gains active role. No user intervention is needed.
- ISSU (irrespective of chassis type): Stateless :
  - User must explicitly terminate all IPSec sessions by shutting the interfaces, perform ISSU and then reestablish tunnels by enabling the interfaces. No other intervention needed.

Miscellaneous IPSec Support Notes
This section contains miscellaneous important notes about IPSec support on the Cisco ASR 1000 Series Router:

- In the context of an IPSec DVTI connection, the Cisco ASR 1000 Router does not support dynamic download ACL rule (per-user attribute) from the AAA server. For example, the following configurations are not supported:
  
cisco-avpair += "ip:inacl#1=permit ip any 2.2.2.0 0.0.0.255"
cisco-avpair += "ip:outacl#1=permit ip 2.2.2.0 0.0.0.255 any"

- The Cisco ASR 1000 Router does not support the command of "if-state nhrp" in configuring the tunnel.

- The Cisco ASR 1000 Router Dead Peer Detection behavior is different than the pre-defined behavior (i.e. when there is no traffic to be sent, no DPD is sent, while if any traffic to be sent, DPD is sent). A Cisco ASR 1000 Router DPD is sent out regardless there is outbound traffic needs to be sent out.
• The Cisco ASR 1000 Router does not support SA Path MTU on data path.
• The Cisco ASR 1000 Router does not support double ACL in dynamic crypto map.
• VRF without crypto map configured on a physical interface causes dual esp reload on a Cisco ASR 1000 Router.
• The command: `show crypto ipsec sa identity` does not log send and receive error counts.
• The commands: `clear crypto` and `show crypto` on Standby RP are inconsistent with Active RP. At present most of other features disable ‘clear commands’ from Standby RP, but IPSec still allows to clear sa, session etc. from the standby.
• The Cisco ASR 1000 Router does not support Cisco AAA av-pair “cisco-avpair += ip:sub-policy-In=policy1”.
• CLI allows both ikev1 and ikev2 profile configured under the same crypto map, even though it is not supported internally on the ASR 1000 Router.
• For a Cisco ASR 1000 Router, the tunnel protection should be removed first before changing any configuration for tunnel protection.
• The security association (SA) maximum transmission unit (MTU) calculation is based on the interface MTU instead of the IP MTU.
• The Cisco ASR 1000 Series Router currently supports a maximum anti-replay window value of 512. If you attempt to configure a value larger than 512, the Cisco ASR 1000 Series Router defaults back to 512 internally (although the display still shows your user-configured value).
• The Cisco ASR 1000 Series Router does not currently support nested SA transformation such as:
  ```plaintext
crypto ipsec transform-set transform-1 ah-sha-hmac esp-3des esp-md5-hmac
crypto ipsec transform-set transform-1 ah-md5-hmac esp-3des esp-md5-hmac
```
• The Cisco ASR 1000 Series Router does not currently support Cisco IOS Certificate Authority (CA) server features.
• The Cisco ASR 1000 Series Router does not currently support COMP-LZS configuration.
• On Cisco ASR 1000 Series Routers, when configuring GRE over IPSec, it is recommended that you use only the tunnel protection mode on the tunnel interface. Using crypto maps on both the tunnel interface and the physical interface to achieve GRE over IPSec is not the supported method of configuration.
• When using dynamic VTI-based IPSec on a Cisco ASR 1000 Router, if there are multiple remote IPSec endpoints behind the same NAT device, only one of the endpoints has connectivity. In other words, multiple endpoints cannot have connectivity at the same time.

**NAT and Firewall ALG Support on the Cisco ASR 1000 Series Routers**

The *NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers* matrix summarizes Network Address Translation (NAT) and Firewall Application Layer Gateway (ALG) feature support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1.0 and later releases. The matrix lists feature support by release. NAT and Firewall ALG support is cumulative; features introduced in earlier releases continue to be supported in later releases. You can find the matrix at http://www.cisco.com/en/US/docs/routers/asr1000/technical_references/asr1000alg_support.pdf
Important Notes About Cisco IOS XE Release 3.2.1S

This section describes important notes about Cisco IOS XE Release 3.2.1S and later releases.

EzVPN Support on the Cisco ASR 1000 Series Routers

On a ASR Cisco 1000 Router, when an EzVPN session is ended, the EzVPN server sends out a Stop Accounting message. This message does not contain the Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, and Acct-Output-Packets fields. It might cause a disruption of accounting performed on traffic.

Maximum IP MTU for Loopback Interfaces

For loopback interfaces, the maximum IP MTU is now 4000. This is to match the serial interface limits.

Important Notes About Cisco IOS XE Release 3.2.0S

This section describes important notes about Cisco IOS XE Release 3.2.0S and later releases.

Cisco ASR 1001-4XT3

Cisco ASR1001-4XT3 chassis functionality is similar to the SPA-4XT3/E3 with the exception of E3 circuitry in Cisco IOS XE 3.2.0S Release.

SIP Trunk Over TCP

SIP TCP trunk calls may not activate if more than one complete SIP messages were contained in one TCP segment in Cisco IOS XE 3.2.0S Release.

This symptom occurs upon SIP trunk over TCP scenario. SIP ALG currently processes only one complete SIP message in one TCP segment (one complete or one complete plus one incomplete), refer to CSCti56370.

TCP Failover in Hardware High-Availability Mode

TCP failover is not supported in Hardware High-Availability mode. If the active node fails in Hardware High Availability mode and if the network is restored, it may take 5 to 10 minutes for the standby node to become the active node. This is because of the reboot and the peer negotiation delay. If the network is not restored, only the switched over active peer is available. Failover is not possible in this state.

Extended ACL as a WCCP Redirect ACL

The Cisco ASR 1000 Series Router supports the use of an extended ACL as a WCCP redirect ACL. However, the option to specify a port range is not supported.
Important Notes About Cisco IOS XE Release 3.1.1S

This section describes important notes about Cisco IOS XE Release 3.1.1S and later releases.

SIP-40G:SPA-4XT-Serial

Cisco SPA-4XT-Serial was not supported in 3.1.0S when plugged into an ASR1000 with SIP-40. This SPA is supported in Release 3.1.1S on SIP-40 linecard.

For more information, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation, see section for SPA-4XT-Serial SPA in Table 1-4 (SIP and SPA Compatibility for Serial SPAs).


Cisco ASR1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide


Important Notes About Cisco IOS XE Release 3.1.0S

This section describes important notes about Cisco IOS XE Release 3.1.0S and later releases.

Bidirectional Forwarding Detection (BFD)

In Cisco IOS XE Release 3.1.0S, Bidirectional Forwarding Detection (BFD) is no longer supported in IP Base software packages. For BFD support, use the Advanced IP Services or Advanced Enterprise Services packages.

DMVPN Spoke Support

In Cisco IOS XE Release 3.1.0S Cisco ASR 1000 Series Routers do not support the `ip nhrp server-only` command if they act as DMVPN spokes.

Important Notes About Cisco IOS XE Release 2.6.0

This section describes important notes about Cisco IOS XE Release 2.6.0 and later releases.

Per-User Attribute on PPP Virtual Access

In Cisco IOS XE Release 2.6.0 multiple instances of the per-user attribute `Cisco-Avpair=lcp:interface-config=<cmd>` is not supported.

For example:

Cisco-AVPair = lcp:interface-config=ip vrf forwarding vpngreen
Cisco-AVPair= lcp:interface-config=ip unnumbered loopback2
Should be configured like this in Cisco IOS XE Release 2.6.0:
Cisco-AVPair = lcp:interface-config=ip vrf forwarding vpngreen
ip unnumbered loopback2

“Multiple instances will be supported in Cisco IOS XE Release 2.6.1”

Legacy QoS Command Deprecation: Hidden Commands

To streamline Cisco IOS QoS (quality of service), certain commands are being hidden. Although these commands are available in Cisco IOS XE Release 2.6, the CLI interactive help does not display them. If you attempt to view a command by entering a question mark at the command line, the command does not appear. However, if you know the command syntax, you can enter it. The system will accept the command and return a message explaining that it will soon be removed. These commands will be completely removed in a future release, which means that you will need to use the appropriate replacement commands.

For more information, see the following document:

VRF-Aware NAT

Dependency of NAT on VFR
ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.5.0

This section describes important notes about Cisco IOS XE Release 2.5.0 and later releases.

Embedded Packet Capture

The Embedded Packet Capture (EPC) feature is not functional and not supported for the Cisco ASR 1000 Series Routers.

QoS - Policing Support for GRE Tunnels

When queuing feature on the GRE tunnel interface is not supported with crypto configured on the physical interface.

QoS: QoS support for GRE/sVTI Tunnel

With IOS XE 2.5.0, the Cisco ASR 1000 Router Series supports Quality-of Service (QoS) applied to
- A GRE or sVTI tunnel with policing and marking only for INGRESS traffic
Important Notes

A GRE or sVTI tunnel with 2-level hierarchy allowing queuing on the second level for EGRESS traffic

When there are multiple egress physical interfaces for a tunnel, and the tunnel target physical interface changes as a result of tunnel target destination route change, either manually by user configuration or by routing protocol, IOS will not prevent the tunnel traffic from moving to an alternate egress physical interface. However, in IOS XE 2.5.0, QoS tunnel move feature is not supported. When tunnel traffic moved to an alternate egress physical interface, tunnel QoS policy may enter a suspended state. At this point, the tunnel QoS policy will have to be removed and reapplied to the tunnel interface for it to take effect. In addition, queuing features on the GRE tunnel interface are not supported when IPSec is configured on the physical interface.

VRF-Aware NAT

Integrating NAT with MPLS VPNs

This section provides information about integrating NAT with MPLS VPNs.

Prerequisites for integrating NAT with MPLS VPNs

Before performing the tasks in this module, you should be familiar with the concepts related to configuring NAT for IP address conservation. All access lists required for use with the tasks in this module should be configured prior to beginning the configuration task. For information about how to configure an access list, see IP Access List Sequence Numbering at the following location:


Note If you specify an access list to use with a NAT command, NAT does not support the commonly used permit ip any command in the access list.

Restrictions for Integrating NAT with MPLS VPNs

- The following functionality is not supported for VRF-Aware NAT:
  - VPN to VPN translations. In other words, VRF cannot be applied on the NAT outside interface.
  - Translation of multicast packets
  - Translations with inside destinations
  - Reversible route maps
  - MIBs
  - MPLS traffic engineering
- Configuring inside dynamic translations defined with outside interface mappings is not supported.
- Configuring inside static translations with interface mappings is not supported. The following commands, which do not include VRF, are not supported:
  - ip nat inside source static esp local-ip interface type number
  - ip nat inside source static local-ip global-ip route-map name
  - ip nat inside source static local-ip interface type number
  - ip nat inside source static tcp local-ip local-port interface type number global-port
  - ip nat inside source static udp local-ip local-port interface type number global-port
Dependency of NAT on VFR
ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.3.0
This section describes important notes about Cisco IOS XE Release 2.3.0 and later releases.

Any Transport Over MPLS (AToM) Support
The configuration of Any Transport Over MPLS (AToM) on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.3.0 is only supported on a subinterface; AToM cannot be configured on the main interface. In addition, you cannot have any IP configuration on the main interface when you have an AToM configuration on the subinterface. These configuration guidelines are applicable to VC mode, VP mode, and L2VPN PW redundancy.

MPLS TE Support
Cisco ASR 1000 Series Router users considering the implementation of MPLS TE are recommended to consult with their local Cisco technical support representative for Cisco IOS XE implementation details.

VRF-Aware NAT

Dependency of NAT on VFR
ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes About Cisco IOS XE Release 2.2.2
This section describes important notes about Cisco IOS XE Release 2.2.2 and later releases.

SSO for L2TP Tunnel Switching Not Supported
If dual route processors (RPs) are used on the Cisco ASR 1000 Series Router in Cisco IOS XE Release 2.2.2 and L2TP Tunnel Switching is configured, then no l2tp sso enable must be configured.

VRF-Aware NAT

Dependency of NAT on VFR
ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces and environments in Cisco IOS XE Release 2.2.2. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.
Important Notes About Cisco IOS XE Release 2.2.1

This section describes important notes about Cisco IOS XE Release 2.2.1 and later releases.

100M FX SFP Not Supported on Cisco 2-Port Gigabit Ethernet Shared Port Adapter

The 100M FX SFP is not supported on the Cisco 2-Port Gigabit Ethernet Shared Port Adapter (2x1GE SPA) on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2.1.

Intelligent Service Gateway (ISG) Features Not Supported

The following Intelligent Service Gateway (ISG) features are not supported on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2.1:

- ISG IP subscriber functionality on the following types of access interfaces: Gigabit EtherChannel (GEC) (Port Channel), generic routing encapsulation (GRE), PPP (virtual-template), and Layer 2 Tunneling Protocol (L2TP)
- ISG prepaid billing
- ISG IP interface sessions
- Interface statistics for ISG multiservice interfaces
- Access lists cannot be configured as match criteria in ISG Layer 4 redirect configuration. As an alternative, Layer 4 redirect should be configured in ISG traffic class services.
- Stateful Switchover (SSO and in-service software upgrade (ISSU) for ISG IP subscriber sessions or traffic class sessions. Upon switchover, an IP session must be recreated or restarted (for Dynamic Host Configuration Protocol (DHCP) sessions) when the session becomes active again.
- SSO and ISSU for any features on IP subscriber sessions or traffic class sessions
- SSO and ISSU for the following features on ISG PPP sessions:
  - Port-Bundle Host Key
  - Layer 4 Redirect
  - Traffic Class

Per-Session Multicast Support

Enhancements to the IP multicast feature provide support for per-session multicast in broadband environments in Cisco IOS XE Release 2.2.1.

VRF-Aware NAT

Dependency of NAT on VFR

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces and environments in Cisco IOS XE Release 2.2.1. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.
Important Notes About Cisco IOS XE Release 2.1.1

This section describes important notes about Cisco IOS XE Release 2.1.1 and later releases.

Startup Configuration File Backup

As a matter of routine maintenance on any Cisco router, users should backup the startup configuration file by copying the startup configuration file from NVRAM onto one of the router’s other file systems and, additionally, onto a network server. Backing up the startup configuration file provides an easy method of recovering the startup configuration file in the event the startup configuration file in NVRAM becomes unusable for any reason.

For users using any Cisco ASR 1000 Series Router with a single RP, including any Cisco ASR 1002 or Cisco ASR 1004 Router, backing up the startup configuration file onto another router file system is especially important due to CSCsq70140, which is documented in the Caveats section of these release notes. The workaround for users who run into this caveat is to replace the startup configuration file in NVRAM with a backup copy of the startup configuration file on the router; therefore, customers who have backed up their startup configuration files onto the router will be ready to resolve these caveats if they occur on their Cisco ASR 1000 Series Routers using a single RP.

Example 1: Copying Startup Configuration File to Bootflash

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 May 29 2008 16:31:41 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
12 -rw- 208904396 May 28 2008 16:17:34 -07:00 asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin

Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]? 

3517 bytes copied in 0.647 secs (5436 bytes/sec)

Example 2: Copying Startup Configuration File to USB Flash Disk

Router# dir usb0:
Directory of usb0:/

43261 -rwx 208904396 May 27 2008 14:10:20 -07:00 asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin

255497216 bytes total (40190464 bytes free)
Example 3: Copying Startup Configuration File to a TFTP Server

```
Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.17.16.81
Destination filename [pe24_asr-1002-config]? /auto/tftp-users/user/startup-config
!!
3517 bytes copied in 0.122 secs (28828 bytes/sec)
```

VRF-Aware NAT

**Dependency of NAT on VFR**

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

**Important Notes About Cisco IOS XE Release 2.1.0**

This section describes important notes about Cisco IOS XE Release 2.1.0 and later releases.

**High-Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers**

Table 1 describes some of the high-level feature sets that are not supported for the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1.0 and later releases. Use Cisco Feature Navigator to confirm support for a specific feature. To access Cisco Feature Navigator, go to [http://www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

Feature support is subject to change from release to release. Some high-level feature sets that were not supported in the initial Cisco IOS XE Release 2.1.0 are now supported. Table 1 has been updated to indicate when support has been introduced in later releases. For the latest feature information, see the New and Changed Information sections of these release notes and Cisco Feature Navigator.
### Table 1: High-Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers

<table>
<thead>
<tr>
<th>Major Feature Category</th>
<th>Feature Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>Support for ATM features begins in Cisco IOS XE Release 2.3.0. No ATM features are supported in earlier releases.</td>
</tr>
<tr>
<td>Broadband</td>
<td>Support for ANCP begins in Cisco IOS XE Release 2.4.0. ANCP is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>IPv6 Intelligent Service Gateway (IPv6 ISG)</td>
</tr>
<tr>
<td></td>
<td>MLP over ATM (MLPoATM)</td>
</tr>
<tr>
<td></td>
<td>MLP over Ethernet (MLPoE)</td>
</tr>
<tr>
<td></td>
<td>Multilink PPP on L2TP Network Server (MLPPP on LNS)</td>
</tr>
<tr>
<td></td>
<td>Point-to-Point Protocol over Ethernet Tag (PPPoE Tag)</td>
</tr>
<tr>
<td></td>
<td>PPP over Q-in-Q (PPPoQinQ)</td>
</tr>
<tr>
<td>Ethernet OAM</td>
<td>Ethernet Operation, Administration, and Maintenance (OAM)</td>
</tr>
<tr>
<td>MPLS</td>
<td>Support for Carrier’s Carrier begins in Cisco IOS XE Release 2.2.3. Carrier’s Carrier is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>Support for Ethernet over MPLS (EoMPLS) begins in Cisco IOS XE Release 2.4.0. Ethernet over MPLS (EoMPLS) is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>Support for Inter-AS begins in Cisco IOS XE Release 2.2.2. Inter-AS is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>IPv6 Provider Edge Router over MPLS (6PE)</td>
</tr>
<tr>
<td></td>
<td>IPv6 VPN over MPLS (6VPE)</td>
</tr>
<tr>
<td></td>
<td>Label Distribution Protocol (LDP) Session Protection</td>
</tr>
<tr>
<td></td>
<td>Support for Layer 2 VPN (L2VPN) begins in Cisco IOS XE Release 2.3.0. L2VPN is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>Support for MPLS Traffic Engineering/Fast Reroute (MPLS TE/FRR) begins in Cisco IOS XE Release 2.3.0. MPLS TE/FRR is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>Virtual Private LAN Service (VPLS)</td>
</tr>
<tr>
<td>Multicast</td>
<td>Multicast VPN</td>
</tr>
<tr>
<td>Routing</td>
<td>Performance Routing/Optimized Edge Routing (PFR/OER)</td>
</tr>
<tr>
<td>Security</td>
<td>Support for Group Encrypted Transport VPN (GET VPN) begins in Cisco IOS XE Release 2.3.0. GET VPN is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>IPv6 IPSec</td>
</tr>
<tr>
<td></td>
<td>Support for Lawful Intercept begins in Cisco IOS XE Release 2.4.0. Lawful Intercept is not supported in earlier releases.</td>
</tr>
<tr>
<td></td>
<td>VRF-Aware Firewall</td>
</tr>
<tr>
<td></td>
<td>Support for VRF-Aware NAT when running ASRNAT this will not handle fragmented packets unless VFR is configured on all NAT interfaces.</td>
</tr>
<tr>
<td>Voice</td>
<td>Support for Cisco Unified Border Element (SP Edition) begins in Cisco IOS XE Release 2.4.0. Cisco Unified Border Element (SP Edition) is not supported in earlier releases. Earlier releases include support for Integrated Session Border Controller.</td>
</tr>
</tbody>
</table>
New Features in and Important Notes About Cisco IOS XE 3.1S Releases

This chapter provides information about the new features introduced in the Cisco IOS XE 3.1S releases. In addition, important notes about these releases are included in this chapter.

Cisco IOS XE 3S releases inherit all Cisco IOS XE Release 2 features that were released prior to the introduction of the Cisco IOS XE 3.1S releases with few exceptions. For information about inherited features that were introduced in Cisco IOS XE Release 2 releases, for a list of new and changed features, and important notes that apply to Cisco IOS XE Release 2, see the “New and Changed Information” section in Cisco IOS XE Release 2 Release Notes.

This chapter contains the following sections:

- New and Changed Information, page 175
- Important Notes, page 193

New and Changed Information

This section lists the new hardware and software features that are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.1S and contains the following sections:

- New Hardware Features in Cisco IOS XE Release 3.1.4S, page 176
- New Software Features in Cisco IOS XE Release 3.1.4S, page 176
- New Hardware Features in Cisco IOS XE Release 3.1.3S, page 176
- New Software Features in Cisco IOS XE Release 3.1.3S, page 176
- New Hardware Features in Cisco IOS XE Release 3.1.2S, page 176
- New Software Features in Cisco IOS XE Release 3.1.2S, page 176
- New Hardware Features in Cisco IOS XE Release 3.1.1S, page 176
- New Software Features in Cisco IOS XE Release 3.1.1S, page 176
- New Hardware Features in Cisco IOS XE Release 3.1.0S, page 179
- New Software Features in Cisco IOS XE Release 3.1.0S, page 181
New Hardware Features in Cisco IOS XE Release 3.1.4S

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.1.4S.

New Software Features in Cisco IOS XE Release 3.1.4S

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.1.4S.

New Hardware Features in Cisco IOS XE Release 3.1.3S

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.1.3S.

New Software Features in Cisco IOS XE Release 3.1.3S

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.1.3S.

New Hardware Features in Cisco IOS XE Release 3.1.2S

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.1.2S.

New Software Features in Cisco IOS XE Release 3.1.2S

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.1.2S.

New Hardware Features in Cisco IOS XE Release 3.1.1S

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.1.1S.

New Software Features in Cisco IOS XE Release 3.1.1S

The following new software features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.1.1S. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes.
Flexible NetFlow—Egress Support

Flexible NetFlow Egress allows the user to monitors traffic that the router is transmitting on an interface or subinterface.

For more information, see the following documents:


Flexible NetFlow—Full Flow Support

This feature allows users to enable Flexible NetFlow to collect Flow Records for every packet.

For more information, see the following documents:


Flexible NetFlow—Ingress Support

Flexible NetFlow feature allows users to collect flow records from IPv4 Unicast packet streams on the router.

For more information, see the following documents:


Flexible NetFlow—IPv4 Unicast Flows

Flexible NetFlow feature allows users to collect flow records from IPv4 Unicast packet streams on router.

For more information, see the following documents:

New Features in and Important Notes About Cisco IOS XE 3.1S Releases

Flexible NetFlow—MPLS Egress NetFlow

Flexible NetFlow MPLS Egress accounting feature enables the user to account for Flows exiting from an MPLS network to an IP network. This feature will be useful for capacity planning and account for flows to a data center.

For more information, see the following documents:

Flexible NetFlow—Multiple User-Defined Caches

Flexible NetFlow feature enables the user to define their own records by specifying the key and non-key fields to customize the data collection to your specific requirements.

For more information, see the following documents:

Flexible NetFlow—NBAR Application Recognition

This enhancement of Flexible NetFlow will allow for L7 visibility from NBAR into Flow Records.

For more information, see the following document:

Flexible NetFlow—NetFlow Export over IPv4

This feature allows for Flows records (IPv4, IPv6, etc.) to be exported to the collector over IPv4.

For more information, see the following document:

Flexible NetFlow—NetFlow v9 Export Format

This feature defines a flexible export format for NetFlow defined by RFC 3954 to cover current and future technologies.

For more information, see the following document:
Flexible NetFlow—v5 Export Protocol

This feature defines Netflow v5 export protocol support.  
For more information, see the following document:

Flexible NetFlow—New Flexible NetFlow CLI

For more information, see the following document:

Flexible NetFlow—Output Features on Data Export

This feature provisions QoS and crypto on Flexible NetFlow export packets.  
For more information, see the following document:

Flexible NetFlow—Sampling

Flow samplers are created as separate components in a router's configuration. Flow samplers are used to reduce the load on the device that is running Flexible NetFlow by limiting the number of packets that are selected for analysis. Samplers use either random or deterministic sampling techniques (modes):

- Deterministic—The same sampling position is used each time a sample is taken.
- Random—A randomly selected sampling position is used each time a sample is taken.

Flow sampling exchanges monitoring accuracy for router performance. When you apply a sampler to a flow monitor, the overhead load on the router of running the flow monitor is reduced because the number of packets that the flow monitor must analyze is reduced. The reduction in the number of packets that are analyzed by the flow monitor causes a corresponding reduction in the accuracy of the information stored in the flow monitor's cache. Samplers are combined with flow monitors when they are applied to an interface with the ip flow monitor command.

For more information, see the following document:

New Hardware Features in Cisco IOS XE Release 3.1.0S

The following new hardware features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.1.0S.
Cisco ASR 1013 Router

The Cisco ASR 1013 router extends the Cisco ASR 1000 Series Routers to a chassis that can hold six SIPs and provides superslots (more height and power) for the Cisco ASR1000-RPs (route processor) and the ASR1000-ESPs (forwarding processor).

The Cisco ASR 1013 Router is a 24-SPA,3-rack-unit (RU), hardware-redundant chassis with two Embedded Services Processor (ESP) slots, two Route Processor (RP) slots, and six SIP slots that allows for full Route-Processor hardware redundancy, NSF, ISSU, and future Route-Processor service upgrades.

For information about the Cisco ASR 1013 Router, see Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide at the following location:


Field Programmable Hardware Device Upgrade

Beginning with Cisco IOS XE Release 3.1.0S, Cisco ASR 1000 Series Routers have the capability to allow users to perform upgrades in the field on programmable hardware devices. Field programmable hardware devices include the Complex Programmable Logic Device (CPLD) and the field programmable gate array (FPGA). In Cisco IOS XE Release 3.1.0S and later releases, a CPLD field upgrade is required to upgrade incompatible versions of firmware on the Cisco ASR1000-RP2 and Cisco ASR1000-SIP10 components in the Cisco ASR 1013 Router. A hardware programmable package is released to customers for the CPLD upgrade.

For more information, see Upgrading Field Programmable Hardware Devices for Cisco ASR 1000 Series Routers.

New Embedded Services Processors

Cisco IOS XE Release 3.1.0S introduces support for the following new Embedded Services Processors (ESPs):

The Cisco ASR1000-ESP40 is a 40Gbps, QFP-based forwarding processor for the Cisco ASR 1000 Series Aggregation Services Router platform.

- See Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide at the following location:
  

- See Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide at the following location:
  

- For information about the ASR1000-ESP40, see Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide at the following location:
  
New and Changed Information

While both the Cisco ASR1000-ESP40 and ASR1000-ESP20 exceed the 16 Mbps forwarding rate, the ASR1000-ESP40 packets per second rate is slightly less than ASR1000-ESP20 when sending continuous stream of small, 64-byte packets. However, at 92 bytes and larger, the ASR1000-ESP40 outperforms the Cisco ASR1000-ESP20. The difference at small packet sizes is a side-effect of optimizations made to achieve 40 Gbps for medium to large packets.

New Software Features in Cisco IOS XE Release 3.1.0S

The following new software features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 3.1.0S. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes.

1+1 SR-APS Without Bridging

1+1 Single Router APS without Bridging feature is used when asserting LAIS on a non-active link. For more information, see the following document:

6PE Multipath

This feature allows for multipath (load balancing) support on 6PE. For more information, see the following document:

Additional PDL Support for NBAR

The following PDL support will be updated/added: Youtube/dicom/cifs/Aim/msn/Sap/Vnc/Softphone + skinny parity/Mapi pdl/Bittorrent/Gnutella/Skype/Winmx parity/Sip parity/Cifs For more information, see the following document:

BGP—Remove/Replace Private AS Filter

BGP - Remove/Replace Private AS Filter feature provides the ability for customers to remove/replace Private AS Numbers in the as-path from outgoing BGP updates. For more information, see the following document:

BGP Dynamic Neighbors

BGP Dynamic Neighbors allow for configuration of prefix ranges which should accept incoming TCP sessions and dynamically create a BGP neighbor relationship with the source IP.
New and Changed Information

For more information, see the following document:

BGP Slow Peer

BGP Peers belonging to the same update group can be starved of route advertisements/withdrawals if there is a slow peer present in that update group. This feature detects the slow peers and moves them to a new update group so that other non slow peers can accept the update messages.

For more information, see the following document:

Cisco Unified Border Element (Enterprise)

The following Cisco Unified Border (Enterprise) features were introduced in Cisco IOS XE Release 3.1.0S:

- Interworking of Secure RTP calls for SIP and H323
- RFC4040 based Clear Channel Codec Signaling with SIP
- Session Border Controller Enhancements for H.323-SIP and SIP-SIP Supplementary Services, Transcoding Optimization and Firewall Integration.
- SIP-SIP Basic Feature Functionality for Session Border Controller (SBC)
- SIP-SIP Extended Feature Functionality for Session Border Controller (SBC)
- SIP-Support for SIP Video Calls with Flow Around Media
- SIP Diversion Header Enhancements
- SIP History INFO
- SIP SRTP Fallback to Nonsecure RTP for CUBE
- SIP to SIP Supplementary Services for Session Border Controller (SBC)
- SIP Video Support for Telepresence Calls
- SIP Gateway Support for the bind Command
- Support Ability to Configure Source IP Address for Signaling and Media per SIP Trunk
- Support for Configurable Pass-through of SIP INVITE Parameters
- Support for Configuring Error Response Code Upon Out-of-dialog OPTIONS Ping Failure
- Support for dynamic payload type interworking for DTMF and codec packets for SIP to SIP calls
- Support for Expires timer reset on receiving or sending SIP 183 message
- Support for generating Out-of-dialog SIP OPTIONS Ping messages to monitor SIP Servers
- Support for interworking between RSVP capable and RSVP incapable networks
- Support for MIB to report call volume and call rate related statistics on the Cisco Unified Border Element
- Support for Multiple Registrars on SIP Trunks on a Cisco Unified Border Element, on Cisco IOS SIP TDM Gateways, and on Cisco Unified Communications Manager Express
• Support for PAI, PPI, Privacy, P-Called-Party-ID and P-Associated-URI headers on Cisco Unified Border Element
• Support for selective filtering of outgoing provisional responses
• Support for SIP 181 'call is being forwarded' message
• Transparent Tunneling of QSIG and Q.931 over SIP-SIP Cisco Unified Border Element

For information about these Cisco Unified Border Element (Enterprise) features, see the following documents:
Cisco Unified Border Element (Enterprise) Configuration Guide:

Cisco Unified Border Element (Enterprise) Configuration Guide: SIP Trunking for PSTN Access:

Cisco Unified Border Element (Enterprise) Configuration Guide: SIP-to-SIP Connections on a Cisco Unified Border Element:

Cisco Unified Border Element (SP Edition)—Unified Model

The following Cisco Unified Border Element (SP Edition) features were introduced in Cisco IOS XE Release 3.1.0S:
• Call-routing: Customized System Error Messages
• Call-routing: ENUM Client
• DBE:Ia Profile: Allow b line parameter to be optional
• DBE:Ia Profile: ETSI BGF Profile support
• IMS: Rx Support
• IMS: Subscribe to Users Registration state
• Media: Asymmetric Payload-Type pass-through in both signaling (SIP/H.323) and media (RTP)
• Media: DTMF method interworking and ACCEPT header handling
• Media: SRTP to RTP support
• Regulation-Compliance: CALEA IRI interface support
• Release 3.1.0 General Enhancements
• SIP Destination ID & SIP Source ID handling
• SIP: IPv6 VRF Support
• SIP: Redundant Signaling Peer
• SIP: Support re-offer of a dynamic codec without an rtpmap present in the re-offered SDP

For information about these Cisco Unified Border Element (SP Edition) features, see the following documents:
New and Changed Information


For information about these Cisco Unified Border Element (SP Edition) Distributed Model features, see the following documents:

Cisco Unified Border Element (SP Edition) Configuration Guide: Distributed Model
Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model

DHCP—Relay Option 82 Encapsulation

IOS DHCP relay is enhanced to add an encapsulated option 82. Encapsulated option 82 is a composite option 82 created from the existing option 82 in the received DHCP message plus new information added by the IOS DHCP Relay.

For more information, see the following documents:


DHCP—Server User Authentication

The DHCP Server offers user authentication. An IP address is handed out if the requestor client authenticated itself.

For more information, see the following document:


Embedded Event Manager (EEM) 3.0

The Cisco IOS Embedded Event Manager is an infrastructure feature that provides unique customization capabilities and event driven automation within Cisco products.

For more information, see the following documents:


Enable NAT High-Speed Logging per VRF

The feature provides the user with a means to turn on/off ASR NAT High-Speed Logging on a per VRF basis.

For more information, see the following document:

Event MIB and Expression MIB Enhancements

This feature provides RFC support for the Expression MIB and a command line user interface for configuring the Event and Expression MIBs.

For more information, see the following document:

Firewall—NetBIOS ALG Support

For more information, see the following document:

Firewall—GPI (Granular Protocol Inspection) Phase-2 Support

Firewall: GPI (Granular Protocol Inspection) Phase-2 feature enables support for additional protocols.

Firewall Stateful Inter-Chassis Redundancy

For more information, see the following document:

HSRP for IPv6

Hot-Stand By Router Protocol (HSRP) for IP version 6 (IPv6). HSRP for IPv6 uses link local addresses and is compatible with IPv6 MPLS VPN (6VPE) when available.

For more information, see the following document:

Ingress Packet Scheduling (Intra-CC and Inter-CC Ingress Scheduling)

This feature allows for ingress packet scheduling applicable to packets entering the ASR 1000 Router through an interface.

For information about Ingress Packet scheduling (both intra-CC & inter-CC ingress scheduling) and other SPAs supported on the Cisco ASR 1000 Series Routers, see the following document:
Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide at:

Input Packet Classification on SPA Interface Processor (SIP) Card

The feature allows for input packet classification at the Carrier Card based on various packet types and fields.
New and Changed Information

For information about Input packet classification on SPA Interface Processor card (SIP) and other SPAs supported on the Cisco ASR 1000 Series Routers, see the following document:
Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide at:

**IP Tunneling, 6RD IPv6 Rapid Deployment**

This feature implements 6RD draft and allows cost effective deployment of IPv6 over IPv4 core using v6 over v4 tunneling mechanism. This is an extension of 6 to 4 feature support.

For more information, see the following document:

**IPv6 Switching—Provider Edge Router over MPLS (6PE)**

This feature provides a method of sending IPv6 packets originating from an IPv6 Edge router across an MPLS network backbone running an IPv4 control plane, without making changes to the software on the MPLS PE routers.

For more information, see the following document:

**IPv6 VPN over MPLS (6VPE)**

IPv6 VPN features over a MPLS/IPv4 core infrastructure (6VPE), includes IPv6 VRF-Lite support.

For more information, see the following document:

**IPv6 VPN over MPLS (6VPE) Inter-AS options**

IPv6 VPN features over a MPLS/IPv4 core infrastructure (6VPE), includes Inter-AS option a, b, c support.

For more information, see the following document:

**IPv6—NSF and Graceful Restart for MP-BGP IPv6 Address Family**

For more information, see the following document:
New and Changed Information

ISG—Authentication: DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

ISG needs to support option 60/82 based TAL for provisioning per service QoS and VPN-ID sub-option for provisioning IP wholesale services. Currently IP Sessions cannot differentiate between devices behind a Layer3 CPE for. By adding Option 60 support, IP sessions can be set up for PCs and set top boxes separately, for example.

For more information, see the following documents:

ISSU—BGP NSR (Nonstop Routing)

BGP Nonstop Routing (NSR) maintains BGP sessions and state information across ISSU support on a PE device providing MPLS VPN services.

For more information, see the following document:

ISSU—HSRPv6 on VRF Interfaces

This feature enables ISSU Support on HSRPv6 feature on VRF interfaces.

For more information, see the following documents:

MPLS TE—RSVP Graceful Restart 12.0S-12.2S Interoperability

This feature provides support for per-node RSVP Graceful Restart Hello’s in 12.2S IOS release, to allow interoperability with 12.0S IOS.

For more information, see the following document:

MPLS VPN—BGP Local Convergence

This feature allows a MPLS VPN PE router to forward temporarily MPLS VPN packets received from the MPLS core via another PE temporarily when the local PE-CE link goes down. This improves end to end VPN traffic loss as the connectivity reestablishment does not depend on BGP network convergence over the MPLS/IGP core.

For more information, see the following documents:
New Features in and Important Notes About Cisco IOS XE 3.1S Releases

**MPLS VPN—BGP Local Convergence for 6VPE/6PE**

For more information, see the following document:


**MPLS VPN 6VPE Support Over IP Tunnels**

This functionality allows operators to provide 6VPE functionality over GRE tunnel instead of using MPLS LSP to reach the BGP nexthop (remote PE).

For more information, see the following document:


**MPLS VPN over mGRE**

This feature allow for the ability to carry MPLS Layer 3 VPN traffic over mGRE.

For more information, see the following document:


**NAT—Improved Pool Scaling**

NAT now supports 1200 overloaded single range pools.

**NAT—NetBIOS ALG Support**

This features allows NAT to be a part of NetBIOS ALG support.

For more information, see the following document:


**NAT—Real Time Streaming Protocol (RTSP) Support**

This features adds RTSP NAT ALG support.

For more information, see the following document:


**NAT Stateful Inter-Chassis Redundancy**

This feature allows for NAT Stateful Inter-Chassis redundancy support.

For more information, see the following document:


**NBAR PDLM Feature Supported**

Classifying Network Traffic Using NBAR in Cisco IOS XE Software.
For more information, see the following document:

**NBAR Static IPv4 IANA Protocols**

This feature allows NBAR to detect with classify a set of Protocol & Applications standardized by IANA.
For more details about this list, go to http://www.cisco.com/go/nbar and edit the IANA Protocol Pack1 document.

**NSF/SSO—HSRPv6 on VRF Interfaces**

This feature enables NSF/SSO support for HSRPv6 on VRF interfaces.
For more information, see the following documents:

**NSF/SSO BGP NSR (Non Stop Routing)**

BGP Nonstop Routing (NSR) maintains BGP sessions and state information across Stateful SwitchOver (SSO) functions.
For more information, see the following documents:

**Product Security Baseline: Password Encryption and Complexity Restrictions**

For more information, see the following document:

**QoS—Egress Service Policy 3 level Hierarchy (IPv4)**

The QoS: Egress Service Policy 3 level Hierarchy (IPv4) feature supports 3 level policy-map hierarchy with queuing in the leaf level.
The parent level is the top or root level. It supports the default class with shape configured; a user cannot define a class. The parent level supports the following queuing services:
- Shaping
- Bandwidth Remaining Ratio (BRR)
- Shaping and BRR
The child level is the middle level. It supports the following queuing services:
New and Changed Information

- Shaping
- BRR
- Shaping and BRR
- Bandwidth Remaining Percentage (BRP)
- WRED
- Fair Queue

Bandwidth and Priority are supported in a class at the child level as long as the class does not have a queuing policy as a child. This means the class is not directly part of a three level queuing hierarchy.

Users can over-provision shapers at child and parent levels. For example, users can have two child shapers of 50 Mbps and a parent shaper of 75 Mbps.

The grandchild level is the leaf level. It supports queuing services on the following interfaces:
- Physical Interface
- VLAN (GE)
- subinterface (FR or serial)
- GRE tunnel (IPv4)
- sVTI (IPv4)

Mixed queuing and non-queuing features (marking and policing) are supported at the grandchild level.

For more information, see the following document:

**RADIUS Proxy Billing Accuracy**

For more information, see the following document:

**RADIUS VC Logging**

RADIUS Virtual Circuit (VC) Logging allows to accurately record the virtual path interface (VPI) and virtual circuit interface (VCI) of an incoming subscriber session.

For more information, see the following document:

**VASI (VRF-Aware Software Infrastructure) Enhancements Phase I**

VRF-Aware Service Infrastructure (VASI) refers to the capability to use services within different VPN routing and forwarding instances (VRFs). VASI interfaces are virtual interface pairs, where each of the interfaces in the pair is associated with a different VRF.

For more information, see the following document:
New Features in and Important Notes About Cisco IOS XE 3.1S Releases

**VRF-Aware IPsec Phase 2 Support**

This feature allows for IPsec VRF-Aware support for sVTI, Crypto Map-based ezVPN and DMVPN.

For more information, see the following document:


**vTCP for ALG Support**

This feature allows for TCP segment and reassembly support for ALG.

For more information, see the following document:


**WCCP—Configurable Router ID**

This feature allows for the ability to configure the router ID which WCCP will use rather than relying on the router's selection mechanism.

For more information, see the following document:


**WCCP Closed Services**

Permits WCCP services to configured such that the absence of an active client results in intercepted packets being dropped, rather than forwarded.

For more information, see the following document:


**WCCP Increased Services**

This feature increases the number of WCCP services that can be configured from 7 to 256.

For more information, see the following document:


**WCCP Outbound ACL Check**

For more information, see the following document:


**WCCP—Check Services All**

For more information, see the following document:

WCCP—Egress Redirection

For more information, see the following document:

WCCP—Exclude Interface

For more information, see the following document:

WCCP—Fast Timers

The WCCP Fast Timers feature enables WCCP to establish redirection more quickly when a WCCP client is added to a service group or when a WCCP client fails.

WCCP routers and WCCP clients exchange keepalive messages at a fixed interval. Prior to the introduction of the WCCP Fast Timers feature, the WCCP message interval is fixed at 10 seconds. The WCCP Fast Timers feature enables use of message intervals ranging from .5 seconds to 60 seconds and a timeout value scaling factor of 1 to 5.

The WCCP message interval capability introduced by the WCCP Fast Timers feature defines the transmission interval that WCCP clients and WCCP routers use when sending keepalive messages and defines a scaling factor used when calculating the timeout value. The WCCP router uses the timeout value to determine if a WCCP client is no longer available and to redirect traffic as a result.

The WCCP router enforces a single message interval per service group. WCCP clients with incompatible message intervals are prevented from joining a service group.

If a default message interval that is smaller than the default 10 seconds is used, there will be an increase in CPU usage.

You can use the `show ip wccp service-number detail` command to display information about the message interval settings being used in a WCCP service group. No output is displayed if the default 10-second message interval is used.

For more information, see the following document:

WCCP—Group List

For more information, see the following document:

WCCP—Group Listen + Multicast Service

For more information, see the following document:

WCCP—VRF Support

For more information, see the following document:
XML-PI

For customers and partners needing to remotely adapt and control the behavior of Cisco devices, XML-PI 1.0 provides unambiguous and robust information access and control without the complexity and expense of screen-scraping technologies or external XML-to-CLI gateways.

For more information, see the following document:

Important Notes

The following sections contain important notes about Cisco IOS XE 3.1.0S Releases running on Cisco ASR 1000 Series Routers.

Deferrals

Cisco IOS software images are subject to deferral. We recommend that you view the deferral notices at the following location to determine if your software release is affected:

Field Notices and Bulletins

- Field Notices—We recommend that you view the field notices for this release to determine whether your software or hardware platforms are affected. You can access field notices from http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Important Notes About IPSec Support on the Cisco ASR 1000 Series Router

This section contains important notes about IPSec support on the Cisco ASR 1000 Series Router:

IPSec CLI Support Notes

This section contains important notes about IPSec CLI support on the Cisco ASR 1000 Series Router:

For information about Cisco IOS IPSec commands, see the Cisco IOS Security Command Reference at:

- The **show crypto engine** command, which displays information about the crypto engine, is not currently supported on the Cisco ASR 1000 Series Router. The unsupported **show crypto engine** subcommands include the following:
  - **accelerator** (Shows crypto accelerator information.)
  - **brief** (Shows all crypto engines in the system.)
  - **configuration** (Shows crypto engine configuration.)
Important Notes

- **connections** (Shows connection information.)
- **qos** (Shows QoS information.)

- The Cisco ASR 1000 Series Router does not currently support the display of send and recv error statistics using the `show crypto ipsec sa identity` command.
- The Cisco ASR 1000 Series Router does not support the `clear` and `show crypto` commands on the standby Route Processor (RP) by design.
- Counters in the `show platform software ipsec fp active flow identifier n` command are flagged for reset on read. You can use the `show crypto ipsec sa` command to obtain integral counters.
- The `show access-list` command output does not show a packet count matching the ACL.
- The Cisco ASR 1000 Series Router displays debugging information about the consumption of IPsec datapath memory; use the `show platform hardware qfp act feature ipsec datapath memory` command in privileged EXEC or diagnostic mode.
- The Cisco ASR 1000 Series Router displays debugging information about the crypto engine processor registers; use the `show platform software ipsec f0 encryption-processor registers` command in privileged EXEC or diagnostic mode.

Crypto Map Support
This section contains important notes about IPSec crypto map support on the Cisco ASR 1000 Series Router:

- The Cisco ASR 1000 Series Router does not currently support IPSec tunnel configuration for crypto maps with same IP address on both the tunnel interface and the physical interface. Configurations with different IP addresses are supported.
- A possible Embedded Services Processor (ESP) reload may occur if a large number (such as 2000) of crypto maps are removed simultaneously. When removing a large number of crypto maps, it is recommended you unconfigure 500 crypto maps at a time and wait 25 seconds between operations.
- The Cisco ASR 1000 Series Router does not support the `show access-lists id` command under crypto maps.
- The Cisco ASR 1000 Series Router does not currently support the `interface range` command when configuring crypto maps.

IPSec Packet Processing
This section contains important notes about IPSec packet processing on the Cisco ASR 1000 Series Router:

- Reloading an Embedded Services Processor (ESP) on the Cisco ASR 1000 Series Router may cause a few IPSec packets to drop before the initialization completes, but the traffic will resume after a brief interval.
- The Cisco ASR 1000 Series Router will not discard an incoming IP datagram containing a Payload Length other than 4 in the authentication header (AH). For example, a 96 bit authentication value plus the 3 32-bit word fixed portion for any non-null authentication algorithm will not be discarded.
- The Cisco ASR 1000 Series Router does not forward incoming authenticated packets with the IP option field set.

Group Encrypted Transport VPN Support on Cisco ASR 1000 Series Routers
When Group Encrypted Transport VPN is configured on a router, the "deny udp any any port=848" ACL rule is not added by default. You must manually add this rule in the Key Server ACL or Group Member ACL.
Important Notes

GET VPN Support
This section contains important notes about Group Encrypted Transport VPN (GET VPN) support on the Cisco ASR 1000 Series Router:

- In Cisco ASR 1000 series router, group member policies downloaded from key server are treated as shared policy among all group members. So, it does not use the “reversed” policy to check for ingress packet. This behavior is different from other (Cisco7200/ISR) platform. To enable the same behavior as (Cisco 7200/ISR), use the `platform ipsec gdoi accept-both` command in global configuration mode. To disable, use the no form of this command as follows:

  ```
  platform ipsec gdoi accept-both
  no platform ipsec gdoi accept-both
  ```

- Cisco ASR 1000 group member starts re-registration immediately when the local policies are modified. If user adds or removes multiple policies, then re-registration happens with every policy change.

- To ensure normal traffic flow for a GET VPN configuration on a Cisco ASR 1000 series router, a Time Based Anti Replay (TBAR) window-size of greater than 42 seconds is recommended.

- The Cisco ASR 1000 series router does not currently support the TBAR statistics display in the `show crypto gdoi gm replay` command.

- If a Cisco ASR 1000 group member receives empty rekey message from key server, then it loses all its security associations.

- The Cisco ASR 1000 series router does not currently support Easy VPN (EzVPN) and GET VPN on the same interface.

- When a Cisco ASR 1000 series router is to apply the same Group Domain of Interpretation (GDOI) crypto maps to two interfaces, you should use local addresses for the crypto maps. Non-local address configuration is not supported.

- The Cisco ASR 1000 series router does not currently support transport mode for TBAR.

- The Cisco ASR 1000 series router only supports the reassembly of post-fragmented GET VPN packets that are destined for the local Cisco ASR 1000 Series Router in the GET VPN network.

- An enhancement is added to enable reassembly of IPsec transit traffic. This enhancement applies only to post-encryption fragmented IPsec packets. When this enhancement is enabled, IPsec will detect transit IPsec traffic and reassemble it before decryption. GET VPN transit IPsec traffic will be reassembled, decrypted, and forwarded to the destination. Non GET VPN transit IPsec traffic will be reassembled but not decrypted (because the ASR 1000 router is not the IPsec tunnel end point) and then forwarded to the destination.

To enable IPsec reassembly of transit traffic, use the `platform ipsec reassembly transit` command in global configuration mode. To disable IPsec reassembly of transit traffic, use the no form of this command as follows:

  ```
  platform ipsec reassembly transit
  no platform ipsec reassembly transit
  ```

IPSec SSO and ISSU Support Notes
- The Cisco ASR 1000 Series Router supports stateful IPSec sessions on ESP switchover. During ESP switchover, all IPSec sessions will stay up and no user intervention is needed to maintain IPSec sessions.
• For an ESP reload (no standby ESP), the SA sequence number restarts from 0. The peer router drops packets that do not have the expected sequence number. User may need to explicitly reestablish IPSec sessions to work around this issue for systems that have a single ESP after an ESP reload. User may experience traffic disruption over the IPSec sessions in such cases for the duration of the reload.

• The Cisco ASR 1000 Series Router currently does not support Stateful Switchover (SSO) IPSec sessions on Route Processors (RPs). The IPSec sessions will go down on initiation of the switchover, but will come back up when the new RP becomes active. No user intervention is needed. User will experience traffic disruption over the IPSec sessions for the duration of the switchover, until the sessions are back up.

• The Cisco ASR 1000 Series Router currently does not support stateful ISSU for IPSec sessions. Before performing an ISSU, users must explicitly terminate all existing IPSec sessions or tunnels prior to the operation and reestablish them post ISSU. Specifically, users must ensure that there are no half-open or established IPSec tunnels present before performing ISSU. To do this, we recommend user do a interface shutdown in the case of interfaces that may initiate a tunnel setup, such as a routing protocol initiating a tunnel setup, or interfaces that have keepalive enabled or where there is an auto trigger for an IPSec session. Traffic disruption over the IPSec sessions during ISSU is obvious in this case.

**Summarizing and restating the different caveats:**

**ESP - switchover (with standby ESP) : Stateful :**
- IPSec sessions should be up. No user intervention needed.

**ESP - Reload (No standby ESP) : Stateless :**
- IPSec sessions will go down and come back up. Usually no user intervention is needed. However, user may need to explicitly reestablish Ipsec session again if anti replay is configured (sequence number checking).

**RP - switchover (with standby RP) : Stateless :**
- IPSec sessions will go down on RP switchover and should reestablish themselves when the new RP gains active role. No user intervention is needed.

**ISSU (irrespective of chassis type): Stateless :**
- User must explicitly terminate all IPSec sessions by shutting the interfaces, perform ISSU and then reestablish tunnels by enabling the interfaces. No other intervention needed.

**Miscellaneous IPSec Support Notes**

This section contains miscellaneous important notes about IPSec support on the Cisco ASR 1000 Series Router:

- The security association (SA) maximum transmission unit (MTU) calculation is based on the interface MTU instead of the IP MTU.

- The Cisco ASR 1000 Series Router currently supports a maximum anti-replay window value of 512. If you attempt to configure a value larger than 512, the Cisco ASR 1000 Series Router defaults back to 512 internally (although the display still shows your user-configured value).

- The Cisco ASR 1000 Series Router does not currently support nested SA transformation such as:

```
crypto ipsec transform-set transform-1 ah-sha-hmac esp-3des esp-md5-hmac
crypto ipsec transform-set transform-1 ah-md5-hmac esp-3des esp-md5-hmac
```

- The Cisco ASR 1000 Series Router does not currently support Cisco IOS Certificate Authority (CA) server features.
Important Notes in Cisco IOS XE Release 3.1S

- The Cisco ASR 1000 Series Router does not currently support COMP-LZS configuration.
- For the Cisco ASR 1000 Series Router, when configuring GRE over IPSec, user is recommended to use only Tunnel protection mode on the Tunnel interface. Using crypto maps on both tunnel and physical interface to achieve GRE over IPSec is not the supported method of configuration.
- The Cisco ASR 1000 Series Router does not currently support VRF-Aware IPSec.

NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers

The NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers matrix summarizes Network Address Translation (NAT) and Firewall Application Layer Gateway (ALG) feature support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1.0 and later releases. The matrix lists feature support by release. NAT and Firewall ALG support is cumulative; features introduced in earlier releases continue to be supported in later releases. You can access the matrix from the following location:


Power Cycling a Cisco ASR 1013 Router

If you are going to power cycle a Cisco ASR 1013 Router, we recommend that you first perform a graceful reload on the router. Power cycling the router without first performing a graceful reload might cause a loss of data stored in the NVRAM. In other words, the configuration file might be lost. Note that this is not observed when a power failure occurs because each active power supply in the two power supply zones is power cycled at the same time during a power failure. If there is a chance that the router might be power cycled without a graceful reload, we recommend that you use the `boot config
file-system:configuration-file nvbypass` command to specify a file system other than the NVRAM for storing the configuration file. The following are examples:

```
Router(config)# boot config harddisk:config_file.cfg nvbypass
Router(config)# boot config bootflash:configuration_data.cfg nvbypass
```

Important Notes in Cisco IOS XE Release 3.1.1S

This section describes important notes about Cisco IOS XE Release 3.1.1S and later releases.

SIP-40G:SPA-4XT-SERIAL

SPA-4XT-SERIAL was not supported in 3.1.0S when plugged into an ASR1000 with SIP-40. This SPA is supported in Release 3.1.1S on SIP-40 linecard.

For more information, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation, see section for SPA-4XT-Serial SPA in Table 1-4 (SIP and SPA Compatibility for Serial SPAs)


Cisco ASR1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide

Important Notes in Cisco IOS XE Release 3.1.0S

This section describes important notes about Cisco IOS XE Release 3.1.0S and later releases.

Bidirectional Forwarding Detection (BFD)

In Cisco IOS XE Release 3.1.0S Bidirectional Forwarding Detection (BFD) is no longer supported in IP Base software packages. For BFD support, use the Advanced IP Services or Advanced Enterprise Services packages.

DMVPN Spoke Support

In Cisco IOS XE Release 3.1.0S Cisco ASR 1000 Series Routers do not support the `ip nhrp server-only` command if they perform as DMVPN spokes.

GDOI Groups

Multiple GDOI groups with the same identity number (for example, 1234) can be configured on a group member as long as a different key server address is specified for each group. This is because both the group identity number and the server address are required to uniquely identify a group on a group member.

GRE Keepalive with Tunnel Protection

The Cisco ASR 1000 Series Router supports GRE keepalive with tunnel protection. However, the keepalive packet that is returned is not encrypted. This limitation is also mentioned in the “Limitations and Restrictions in Cisco IOS XE Release 3.1.0S” section on page 44.

Important Notes in Cisco IOS XE Release 2.6.0

This section describes important notes about Cisco IOS XE Release 2.6.0 and later releases.

Per-User Attribute On PPP Virtual Access

In Cisco IOS XE Release 2.6.0 multiple instances of the per-user attribute ‘Cisco-Avpair=lcp:interface-config=<cmd>’ is not supported.

For example:
Cisco-AVPair = lcp:interface-config=ip vrf forwarding vpngreen
Cisco-AVPair = lcp:interface-config=ip unnumbered loopback2
Should be configured like this in Cisco IOS XE Release 2.6.0:
Cisco-AVPair = lcp:interface-config=ip vrf forwarding vpngreen \ip unnumbered loopback2
“Multiple instances will be supported in Cisco IOS XE Release 2.6.1”
Important Notes in Cisco IOS XE Release 3.1.1S

Legacy QoS Command Deprecation: Hidden Commands

To streamline Cisco IOS QoS, certain commands are being hidden. Although these commands are available in Cisco IOS XE Release 2.6, the CLI interactive help does not display them. If you attempt to view a command by entering a question mark at the command line, the command does not appear. However, if you know the command syntax, you can enter it. The system will accept the command and return a message explaining that it will soon be removed. These commands will be completely removed in a future release, which means that you will need to use the appropriate replacement commands.

For more information, see the following document:

VRF-Aware NAT

Dependency of NAT on VFR
ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes in Cisco IOS XE Release 2.5.0

This section describes important notes about Cisco IOS XE Release 2.5.0 and later releases.

Embedded Packet Capture

The Embedded Packet Capture (EPC) feature is not functional and not supported for the Cisco ASR 1000 Series Routers.

QoS - Policing Support for GRE Tunnels

When queuing feature on the GRE tunnel interface is not supported with crypto configured on the physical interface.

QoS: QoS support for GRE/sVTI Tunnel

With IOS XE 2.5.0, the Cisco ASR 1000 Router Series supports Quality-of Service (QoS) applied to

- A GRE or sVTI tunnel with policing and marking only for INGRESS traffic
- A GRE or sVTI tunnel with 2-level hierarchy allowing queuing on the second level for EGRESS traffic

When there are multiple egress physical interfaces for a tunnel, and the tunnel target physical interface changes as a result of tunnel target destination route change, either manually by user configuration or by routing protocol, IOS will not prevent the tunnel traffic from moving to an alternate egress physical interface.

However, in IOS XE 2.5.0, QoS tunnel move feature is not supported. When tunnel traffic moved to an alternate egress physical interface, tunnel QoS policy may enter a suspended state. At this point, the tunnel QoS policy will have to be removed and reapplied to the tunnel interface for it to take effect.
In addition, queuing features on the GRE tunnel interface are not supported when IPSec is configured on the physical interface.

**VRF-Aware NAT**

**Integrating NAT with MPLS VPNs**

**Prerequisites for integrating NAT with MPLS VPNs**
Before performing the tasks in this module, you should be familiar with the concepts related to configuring NAT for IP address conservation. All access lists required for use with the tasks in this module must be configured before you begin the configuration task. For information about how to configure an access list, see IP Access List Sequence Numbering at the following location:


**Note**
If you specify an access list to use with a NAT command, NAT does not support the commonly used `permit ip any` command in the access list.

**Restrictions for Integrating NAT with MPLS VPNs**

- The following functionality is not supported for VRF-Aware NAT:
  - VPN to VPN translations. In other words, VRF cannot be applied on the NAT outside interface.
  - Translation of multicast packets
  - Translations with inside destinations
  - Reversible route maps
  - MIBs
  - MPLS traffic engineering
- Configuring inside dynamic translations defined with outside interface mappings is not supported.
- Configuring inside static translations with interface mappings is not supported. The following commands, which do not include VRF, are not supported:
  - `ip nat inside source static esp local-ip interface type number`
  - `ip nat inside source static local-ip global-ip route-map name`
  - `ip nat inside source static local-ip interface type number`
  - `ip nat inside source static tcp local-ip local-port interface type number global-port`
  - `ip nat inside source static udp local-ip local-port interface type number global-port`

**Dependency of NAT on VFR**

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

**Important Notes in Cisco IOS XE Release 2.3.0**

This section describes important notes about Cisco IOS XE Release 2.3.0 and later releases.
Any Transport Over MPLS (AToM) Support

The configuration of Any Transport Over MPLS (AToM) on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.3.0 is only supported on a subinterface; AToM cannot be configured on the main interface. In addition, you cannot have any IP configuration on the main interface when you have an AToM configuration on the subinterface. These configuration guidelines are applicable to VC mode, VP mode, and L2VPN PW redundancy.

MPLS TE Support

Cisco ASR 1000 Series Router users considering the implementation of MPLS TE are recommended to consult with their local Cisco technical support representative for Cisco IOS XE implementation details.

VRF-Aware NAT

Dependency of NAT on VFR

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes in Cisco IOS XE Release 2.2.2

This section describes important notes about Cisco IOS XE Release 2.2.2 and later releases.

SSO for L2TP Tunnel Switching Not Supported

If dual route processors (RPs) are used on the Cisco ASR 1000 Series Router in Cisco IOS XE Release 2.2.2 and L2TP Tunnel Switching is configured, then no l2tp sso enable must be configured.

VRF-Aware NAT

Dependency of NAT on VFR

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces and environments in Cisco IOS XE Release 2.2.2. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes in Cisco IOS XE Release 2.2.1

This section describes important notes about Cisco IOS XE Release 2.2.1 and later releases.

100M FX SFP Not Supported on Cisco 2-Port Gigabit Ethernet Shared Port Adapter

The 100M FX SFP is not supported on the Cisco 2-Port Gigabit Ethernet Shared Port Adapter (2x1GE SPA) on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2.1.
Important Notes in Cisco IOS XE Release 3.1S

Intelligent Service Gateway (ISG) Features Not Supported

The following Intelligent Service Gateway (ISG) features are not supported on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2.1:

- ISG IP subscriber functionality on the following types of access interfaces: Gigabit EtherChannel (GEC) (Port Channel), generic routing encapsulation (GRE), PPP (virtual-template), and Layer 2 Tunneling Protocol (L2TP)
- ISG prepaid billing
- ISG IP interface sessions
- Interface statistics for ISG multiservice interfaces
- Access lists cannot be configured as match criteria in ISG Layer 4 redirect configuration. As an alternative, Layer 4 redirect should be configured in ISG traffic class services.
- Stateful Switchover (SSO and in-service software upgrade (ISSU) for ISG IP subscriber sessions or traffic class sessions. Upon switchover, an IP session must be recreated or restarted (for Dynamic Host Configuration Protocol (DHCP) sessions) when the session becomes active again.
- SSO and ISSU for any features on IP subscriber sessions or traffic class sessions
- SSO and ISSU for the following features on ISG PPP sessions:
  - Port-Bundle Host Key
  - Layer 4 Redirect
  - Traffic Class

Per-Session Multicast Support

Enhancements to the IP multicast feature provide support for per-session multicast in broadband environments in Cisco IOS XE Release 2.2.1.

VRF-Aware NAT

Dependency of NAT on VFR

ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces and environments in Cisco IOS XE Release 2.2.1. VFR will automatically be configured when NAT is configured, but users must “not” manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes in Cisco IOS XE Release 2.1.1

This section describes important notes about Cisco IOS XE Release 2.1.1 and later releases.

Startup Configuration File Backup

As a matter of routine maintenance on any Cisco router, users should backup the startup configuration file by copying the startup configuration file from NVRAM onto one of the router’s other file systems and, additionally, onto a network server. Backing up the startup configuration file provides an easy method of recovering the startup configuration file in the event the startup configuration file in NVRAM becomes unusable for any reason.
For users using any Cisco ASR 1000 Series Router with a single RP, including any Cisco ASR 1002 or Cisco ASR 1004 Router, backing up the startup configuration file onto another router file system is especially important due to CSCsq70140, which is documented in the Caveats section of these release notes. The workaround for users who run into this caveat is to replace the startup configuration file in NVRAM with a backup copy of the startup configuration file on the router; therefore, customers who have backed up their startup configuration files onto the router will be ready to resolve these caveats if they occur on their Cisco ASR 1000 Series Routers using a single RP.

**Example 1: Copying Startup Configuration File to Bootflash**

Router# dir bootflash:
Directory of bootflash:/

```
11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 May 29 2008 16:31:41 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
12 -rw- 208904396 May 28 2008 16:17:34 -07:00 asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin
```

Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]?

```
3517 bytes copied in 0.647 secs (5436 bytes/sec)
```

Router# dir bootflash:
Directory of bootflash:/

```
11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 May 29 2008 16:31:41 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
12 -rw- 208904396 May 28 2008 16:17:34 -07:00 asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin
13 -rw- 7516 Jul 2 2008 15:01:39 -07:00 startup-config
```

**Example 2: Copying Startup Configuration File to USB Flash Disk**

Router# dir usb0:
Directory of usb0:/

```
43261 -rwx 208904396 May 27 2008 14:10:20 -07:00 asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin
```

255497216 bytes total (40190464 bytes free)

Router# copy nvram:startup-config usb0:
Destination filename [startup-config]?

```
3172 bytes copied in 0.214 secs (14822 bytes/sec)
```

Router# dir usb0:
Directory of usb0:/

```
43261 -rwx 208904396 May 27 2008 14:10:20 -07:00 asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin
43262 -rwx 7516 Jul 2 2008 15:40:45 -07:00 startup-config
```

255497216 bytes total (40186880 bytes free)
Example 3: Copying Startup Configuration File to a TFTP Server

Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.17.16.81
Destination filename [pe24_asr-1002-config]? /auto/tftp-users/user/startup-config
!!
3517 bytes copied in 0.122 secs (28828 bytes/sec)

VRF-Aware NAT

Dependency of NAT on VFR
ASRNAT will not handle fragmented packets unless VFR is configured on all NAT interfaces. VFR will automatically be configured when NAT is configured, but users must not manually unconfigure VFR on NAT interfaces as NAT cannot process the fragmented packets and out-of-order fragments correctly.

Important Notes in Cisco IOS XE Release 2.1.0

This section describes important notes about Cisco IOS XE Release 2.1.0 and later releases.

High-Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers

Table 1 describes some of the high level feature sets that are not supported for the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1.0 and later releases. Use Cisco Feature Navigator to confirm support for a specific feature. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note: Feature support is subject to change from release to release. Some high-level feature sets that were not supported in the initial Cisco IOS XE Release 2.1.0 are now supported. Table 1 has been updated to indicate when support has been introduced in later releases. For the latest feature information, see the New and Changed Information sections of these release notes and Cisco Feature Navigator.

<table>
<thead>
<tr>
<th>Major Feature Category</th>
<th>Features Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>Support for ATM features begins in Cisco IOS XE Release 2.3.0. No ATM features are supported in earlier releases.</td>
</tr>
<tr>
<td>Broadband</td>
<td>Support for ANCP begins in Cisco IOS XE Release 2.4.0. ANCP is not supported in earlier releases. IPv6 Intelligent Service Gateway (IPv6 ISG) Multilink PPP on L2TP Network Server (MLPPP on LNS) Point-to-Point Protocol over Ethernet Tag (PPPoE Tag) PPP over Q-in-Q (PPPoQinQ)</td>
</tr>
<tr>
<td>Ethernet OAM</td>
<td>Ethernet Operation, Administration, and Maintenance (OAM)</td>
</tr>
</tbody>
</table>
**Table 1  High-Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers (continued)**

<table>
<thead>
<tr>
<th>Major Feature Category</th>
<th>Features Not Supported</th>
</tr>
</thead>
</table>
| **MPLS**               | Support for Carrier’s Carrier begins in Cisco IOS XE Release 2.2.3. Carrier’s Carrier is not supported in earlier releases.  
Support for Ethernet over MPLS (EoMPLS) begins in Cisco IOS XE Release 2.4.0. Ethernet over MPLS (EoMPLS) is not supported in earlier releases.  
Support for Inter-AS begins in Cisco IOS XE Release 2.2.2. Inter-AS is not supported in earlier releases.  
IPv6 Provider Edge Router over MPLS (6PE)  
IPv6 VPN over MPLS (6VPE)  
Label Distribution Protocol (LDP) Session Protection  
Support for Layer 2 VPN (L2VPN) begins in Cisco IOS XE Release 2.3.0. L2VPN is not supported in earlier releases.  
Support for MPLS Traffic Engineering/Fast Reroute (MPLS TE/FRR) begins in Cisco IOS XE Release 2.3.0. MPLS TE/FRR is not supported in earlier releases.  
Virtual Private LAN Service (VPLS) |
| **Multicast**          | Multicast VPN |
| **Routing**            | Performance Routing/Optimized Edge Routing (PFR/OER) |
| **Security**           | Support for Group Encrypted Transport VPN (GET VPN) begins in Cisco IOS XE Release 2.3.0. GET VPN is not supported in earlier releases.  
IPv6 IPSec  
Support for Lawful Intercept begins in Cisco IOS XE Release 2.4.0. Lawful Intercept is not supported in earlier releases.  
VRF-Aware Firewall |
| **Voice**              | Support for VRF-Aware NAT when running ASRNAT this will not handle fragmented packets unless VFR is configured on all NAT interfaces.  
Support for Cisco Unified Border Element (SP Edition) begins in Cisco IOS XE Release 2.4.0. Cisco Unified Border Element (SP Edition) is not supported in earlier releases. Earlier releases include support for Integrated Session Border Controller. |
Caveats in Cisco IOS XE 3.5S Releases

This chapter provides information about caveats in Cisco IOS XE 3.5S releases. Because Cisco IOS XE 3S is based on Cisco IOS XE 2 inherited releases, some caveats that apply to Cisco IOS XE 2 releases also apply to Cisco IOS XE 3S. For a list of the software caveats that apply to Cisco IOS XE 2, see the “Caveats for Cisco IOS XE Release 2” section at the following location:


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


This chapter contains the following sections:

- Caveats in Cisco IOS XE 3.5S Releases, page 207

Caveats in Cisco IOS XE 3.5S Releases

Caveats describe unexpected behavior. 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 this chapter.

This section describes caveats in Cisco IOS XE 3.5S releases.

In this section, the following information is provided for each caveat:

- Symptom—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)
The Dictionary of Internetworking Terms and Acronyms contains definitions of acronyms that are not defined in this document:

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

This section contains the following topic:

- Resolved Caveats—Cisco IOS XE Release 3.5.2S, page 208
- Open Caveats—Cisco IOS XE Release 3.5.1S, page 212
- Resolved Caveats—Cisco IOS XE Release 3.5.1S, page 214
- Open Caveats—Cisco IOS XE Release 3.5.0S, page 231

**Resolved Caveats—Cisco IOS XE Release 3.5.2S**

This section documents the issues that have been resolved in Cisco IOS XE Release 3.5.2S.

- **CSCtu98960**
  Symptoms: The router crashes with scaling of 3500 spokes.
  Conditions: This symptom is observed when scaling to 3500 spokes.
  Workaround: There is no workaround.

- **CSCtx21589**
  Symptoms: The `show interface gig` command is not showing the media type information.
  Conditions: This symptom is observed when executing the `show interface gig` command.
  Workaround: Test SFP details 1-8 will give the media type information.

- **CSCtx31201**
  Symptoms: PfR may have some probe missing after shut/no shut of the PfR master.
  Conditions: This symptom is observed in a scale topology.
  Workaround: There is no workaround.

- **CSCtx35498**
  Symptoms: ASRNAT B2B: sessions are not aged on the active.
  Conditions: This occurs when the standby stays down.
  Workaround: Do not have the standby down for extended time periods.

- **CSCtx37768**
  Symptoms: QoS classification does not match traffic against an egress policy map between MPLS and IP access.
  Conditions: This symptom is observed when a QoS policy is applied on an EVC bridge domain interface.
  Workaround: Use one of the following workarounds:
  - Reload the router.
  - Remove and reapply an encapsulation configuration such as a VLAN.
  - Remove and reattach the bridge domain under the EVC.
  - Perform a `shutdown/no shutdown` on the BDI interface.
• CSCtx45774
Symptoms: The IM module crashes.
Conditions: This symptom is observed when you create a CESoPSN CEM interface.
Workaround: There is no workaround.
Further Problem Description: The IM crash leads to an IM reload. All CESoPSN connections come up in working state after this IM reload.

• CSCtx47195
Symptoms: BFD flap is seen when doing midpoint node SSO.
Conditions: This symptom is observed with BFD sessions running at 6.6ms X3 flaps when doing a soft OIR on a midpoint node through which MPLS-TP BFD sessions run. This issue is seen with 10G and 1G as the NNI interface combination.
Workaround: There is no workaround.

• CSCtx67388
Symptoms: The upstream packet does not flow in the dual-homed PE model.
Conditions: This symptom is observed when packets destined to VRRP MAC do not get redirected and forwarded out when received on the standby VRRP Gateway.
Workaround: There is no workaround.

• CSCtx70505
Symptoms: The Standby FP crashes and gets stuck in INIT standby state after an FP restart.
Conditions: This symptom is observed with BBA client login and logout with high TPS. Run the `show platform software peer chassis-manager fp standby` command periodically.
Workaround: Reload the router.

• CSCtx82775
Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.
Conditions: This symptom is observed when MTP is invoked for calls.
Workaround: Reload the router or perform a no sccp/sccp.

• CSCtx86069
Symptoms: The dynamic NAT has a wrong translation that causes multiple inside local addresses to be translated to the same inside global address.
Conditions: This symptom is observed with the following conditions:
  - Cisco IOS XE Release 3.4.2.
  - Call flow: multiple sip caller -- proxy --(inside)-- ALG --(outside)-- sip callee.
  - Inside dynamic NAT is configured, with one hour timeout.
Steps of reproducing:
1. Make some of the SIPP calls for several hours.
2. After some hours, make calls from idle SIPP.
For the new inside local IP address, NAT will be translated to an existing inside global in the table (without create a new binding in NAT table), which is bound with another inside local address.
Workaround: There is no workaround.
• CSCtx94393
Symptoms: ESP crashes at fman_avl_free.
Conditions: This symptom is observed with the following conditions:
  – Scale IKEv2 4k IPsec sessions with the FlexVPN dVTI server.
  – Scale IKEv1 1k IPsec sessions with the dVTI server.
  – CAC (50) enabled on both the server and client.
  – DPD (60/15/on-demand) enabled.
  – Do a clear crypto session per 20 minutes on the server.
  – 20M bidirectional traffic.
Workaround: There is no workaround.

• CSCtx96285
Symptoms: A configuration of stateful inter-chassis redundancy for NAT may result in packets routing through the standby router and not being processed by the NAT rules, or dropped (NAT is being bypassed).
Conditions: This symptom is observed after a failover of primary to secondary with all routing protocols forcing traffic to the standby router.
Workaround: There is no workaround.

• CSCty17747
Symptoms: On a Cisco ASR 1000 router that contains an ESP40 forwarding card or on a Cisco ASR 1001 router, there is an issue that prevents Traditional Netflow (TNF) exporters configured under the aggregation cache command from being properly created when the router is reloaded and booted from the startup configuration. A typical command snippet would look like:

```
ip flow-aggregation cache prefix
  cache entries 512000
  cache timeout active 5
  export version 9
  export template refresh-rate 5
  export destination 192.168.1.2 9995
  export destination 192.168.3.4 9995
  mask source minimum 32
  mask destination minimum 32
  enabled
```

If this configuration is in the startup configuration and the router is reloaded, the exporter commands will not take effect after the reload and no packets will be exported.

Conditions: This symptom has only been observed on either ESP40 forwarding cards or on a Cisco ASR 1001 router. This issue does not occur during manual configuration but only when the router is reloaded and the startup configuration (or other bootup configuration) is parsed.

Workaround: Reapply the missing exporter configuration manually after the router is already up.

• CSCty31732
Symptoms: Ping fails to the peer end that has a port-channel with member links on different niles. OSPF neighbourship is also not established.
Conditions: This symptom is observed with a port-channel in the core that has member links on different niles.

Workaround: Flap (shut/no shut) the port-channel member links.
• CSCty35010
Symptoms: Interface counters are not proper in the `show interface` command
Conditions: Abnormal interface counters are observed on interfaces that have service-instances configured under them. Also `show interface port-channel` packet in and packet out counters are not equal to the sum of the counters on each member.
Workaround: There is no workaround.

• CSCty43582
Symptoms: The `port-channel load-balance-hash-algorithm` CLI is not saved properly in the running configuration.
Conditions: This symptom is observed when the hash algorithm chosen is one of src-ip, dst-ip, or src-dst-ip.
Workaround: There is no workaround.

• CSCty46022
Symptoms: A Cisco ASR 1000 router experiences high ESP CPU constantly.
Conditions: This symptom is observed when ISG sessions with DHCP initiator are experiencing fragmented traffic and the fragmented traffic has a small packet size. The packets will be puncted to ESP CPU and cause it to be busy.
Workaround: There is no workaround.

• CSCty48439
Symptoms: The `show interface BDI` CLI stats do not increment.
Conditions: This symptom is seen under all conditions.
Workaround: Use the `show platform hardware pp active interface statistics bdi` command to track only valid IPv4 multicast/unicast packets via input and output counts.

• CSCty54885
Symptoms: The Standby RP crashes when the Active RP is removed to do a failover.
Conditions: This symptom is observed when the last switchover happens with redundancy forced-switchover.
Workaround: Do a switchover only with redundancy forced-switchover instead of removing the RP physically.

• CSCty57746
Symptoms: On the Cisco ASR 903 router, the `show environment` command displays incorrect values, including P0 and P1 voltages and Amps values.
Conditions: This symptom is observed with the Cisco ASR 903 router when you apply the `show environment` command.
Workaround: There is no workaround.

• CSCty62559
Symptoms: On the Cisco ASR 1000 series router, FP crash occurs at `cpp_qm_obj_add_to_parent` with 8k xconnects.
Conditions: This symptom is observed with the Cisco ASR 1000 series router while doing SPA reload after RP switchover with 8k xconnects.
Workaround: There is no workaround.
CSCty62887
Symptoms: When more than 1024 DTL requests are made during free sip msg_info pool, the Cisco ASR 1000 router will crash.
Conditions: Multiple factors could contribute to this. It depends on the number of messages contained in SIP ALG.
Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.5.1S
This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.5.1S.

- CSCtx11665
Symptoms: There is a memory leak in the “HTTP CORE” process. Use the sh proc mem sort command to determine the process using the most memory and decode it.
Conditions: This symptom is observed when the default profile is configured on the router, that is, Smart Call Home is enabled.
Workaround 1: In the Smart Call Home profile, use the email transport method to send xml format to backend server. This method needs an available mail server. The reference configuration is below:

```
Router#show run | sec call-home
service call-home
call-home
  contact-email-addr <email address>
  mail-server xxx.xx.xxx.xxx priority 1
  profile "<profile name>"
  active
```
Workaround 2: Disable the default profile so that Smart Call Home is disabled, and then use the http address instead of the https address.

- CSCtx15799
Symptoms: An MTP on a Cisco ASR router sends an “ORC ACK” message through CRC for the channel ID that is just received but does not reply to the ORC for the next channel.
Conditions: This symptom is observed when there is a very short time lapse between the ORC and CRC, say 1 msec.
Workaround: There is no workaround.

- CSCtx25459
Symptoms: An ESP module of a Cisco router may unexpectedly reload due to an exception on the QFP.
Conditions: This symptom is observed when the WCCP connection is reset on a Cisco ASR router configured with WCCP.
Workaround: Disable WCCP.

- CSCtx25926
Symptom: BPDU forwarding stops working on an EOMPLS pseudowire.
Conditions: This symptom is observed in a pseudowire after a change in its core interface.
Workaround: Re-configure the EVC-xconnect.
• **CSCtx32628**
  Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.
  Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:
  - BGP full mesh is configured.
  - BGP cluster-id is configured.
  - `address family vpnv4` is enabled.
  - `address family ipv4 mdt` is enabled.
  - The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.
  Workaround: Remove the cluster-id configuration or hard-reset the bgp session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

• **CSCtx32973**
  Symptoms: A Cisco router crashes due to stack corruption.
  Conditions: This symptom is observed when preemption is seen with the “BFD PP Process” from the crash file similar to the following:

  Preempted processes context:
  ```
  Proc name: BFD PP Process  Preempted PC: 0x6DEF54
  Proc name: BFD PP Process  Preempted PC: 0x6DEBB4
  Proc name: BFD PP Process  Preempted PC: 0x6DEF54
  Proc name: BFD PP Process  Preempted PC: 0x28232D0
  Proc name: BFD PP Process  Preempted PC: 0x28232D0
  Proc name: BFD PP Process  Preempted PC: 0x6DEB7C
  Proc name: BFD PP Process  Preempted PC: 0x6DEBD0
  Proc name: BFD PP Process  Preempted PC: 0x2823280
  Proc name: BFD PP Process  Preempted PC: 0x6FC970
  Proc name: BFD PP Process  Preempted PC: 0x282316C
  ```
  Workaround: There is no workaround.

• **CSCtx37768**
  Symptoms: QoS classification does not match traffic against an egress policy map between MPLS and IP access.
  Conditions: This symptom is observed when a QoS policy is applied on an EVC bridge domain interface.
  Workaround: Use one of the following workarounds:
  - Reload the router.
  - Remove and reapply an encapsulation configuration such as a VLAN.
  - Remove and reattach the bridge domain under the EVC.
  - Perform a `shutdown/no shutdown` on the BDI interface.

• **CSCtx41849**
  Symptoms: A Cisco RP1 crashes during a crypto SS process.
  Conditions: This symptom is observed with the following message under the conditions listed below:
Resolved Caveats—Cisco IOS XE Release 3.5.1S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.5.1S.

- CSCee38838
  Symptoms: A crashdump may occur during a two-call-per-second load test on a gateway, and the gateway may reload.
  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.3(7)T and that functions as a gateway when you run a two-call-per-second load test that uses H.323, VXML, and HTTP. The crash occurs after approximately 200,000 calls.
  Workarounds: There is no workaround.

- CSCsb53810
  Symptoms: A Cisco Catalyst 6500 series switch may not block traffic, which is supposed to be denied by an outbound ACL on a VLAN interface.
  Conditions: This issue is under investigation.
  Workarounds: Reload the switch.

- CSCsg48725
  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.
  Workarounds: Disable AAA. If this not an option, there is no workaround.

- CSCtg57657
  Symptoms: A router is crashing at dhcp function.
  Conditions: This issue has been seen on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T3.
  Workarounds: There is no workaround.

- CSCtg58029
  Symptoms: After switchover, **aaa_acct_session_id** command is not issued to new sessions.
  Conditions: This symptom occurs only after switchover.
Caveats in Cisco IOS XE 3.5S Releases

Workaround: There is no workaround.

- CSCtj64807
  Symptoms: Router crashes while issuing the `show vlans dot1q internal` command.
  Conditions: This symptom is observed with the following conditions:
  1. One QinQ subinterface configured with inner VLAN as “any”.
  2. More than 32 QinQ subinterfaces configured with same outer VLAN.
  3. All subinterfaces are removed except subinterface configured with “any” inner VLAN.
  Workaround 1: For any Cisco 10000 series router which has had its first crash - on any subinterface if the outer VLAN has second-dot1q VLAN as only “any”, immediately delete the sub-interface and recreate it. Then add a dummy VLAN/sub-interface to this outer VLAN.
  Workaround 2: On any outer VLAN (in array state) if they have less than 5 inner VLANs, add a dummy VLAN/subinterface.
  Workaround 3: For any Cisco 10000 series router which has not had a crash but has subinterface/outer VLAN with second-dot1q VLAN as only “any” and active sessions, add a dummy VLAN/sub-interface to this outer (tree state) VLAN.

- CSCtk00181
  Symptoms: Password aging with crypto configuration fails.
  Conditions: This symptom is observed when Windows AD is set with “Password expires on next log on” and the VPN client is initiating a call to NAS. NAS does not prompt for a new password and instead gives an Auth failure.
  Workaround: There is no workaround.

- CSCtk62763
  Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.
  Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.
  Workaround: There is no workaround.

- CSCtn02208
  Symptoms: Old PerUser ACL not removed on applying new ACL.
  Conditions: This symptom occurs when applying a new PerUser ACL to an existing session. The old PerUser ACL that exists on the session is not removed.
  Workaround: There is no workaround.

- CSCtn40771
  Symptoms: The process ACL Header in the `show memory allocating-process totals` command output leaks memory with per-user ACLs and PPP session churn. This will also cause the SSS feature manager process in the `show process memory` command output to appear to have a leak.
  Conditions: This symptom occurs with IPv6 per-user ACLs and session churn.
  Workaround: There is no workaround.

- CSCto71671
  Symptoms: Using the `radius-server source-ports extended` command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.
Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

Workaround: There is no workaround.

- CSCtq59923
  Symptoms: OSPF routes in RIB point to an interface that is down/down.
  Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.
  Workaround: Configure the interface using the `ip routing protocol purge interface` command.

- CSCtr08680
  Symptoms: The following error messages are displayed on active and standby respectively:
  
  %ERROR: Standby doesn’t support this command
  BERT is running on this channel group, please abort bert first.

  Conditions: This symptom is observed when trying to create a channel after BERT has been started irrespective of whether BERT is running or completed.
  Workaround: There is no workaround.

- CSCtr45551
  Symptoms: T1/E1 controller does not get selected as network clock input source.
  Conditions: This symptom occurs when `network-clock input source t1/e1` command is configured immediately after reload of the router or within 5 minutes from router bootup.
  Workaround: After the router reloads, wait for 5 to 6 minutes (until SETS gets initialized) and then configure T1/E1 as network clock input source.

- CSCtr47642
  Symptoms: On Cisco IOS Release 15.2(3)T that is running BGP configured as RR with multiple eGBP and iBGP non-clients and iBGP RR clients and enabling the BGP best-external feature using the `bgp additional-paths select best-external` command, a specific prefix may not have bestpath calculated for a long time.
  Conditions: The problem occurs on a certain condition of configuration of the below commands, and a few prefixes are withdrawn during the configuration time:

  1. Configure: `bgp additional-paths install` under VPNv4 AF.

  Immediately disable backup path calculation/installation using the `no bgp additional-paths install` command.

  The problem does not appear if both of the above commands are configured with more than a 10-second delay as the commands will be executed independently in two bestpath runs instead of one.

  Workaround: Configure the `bgp additional-paths install` command and the `bgp additional-paths select best-external` command with a delay of 10 seconds.

- CSCtr88739
  Symptom 1: The routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.
Symptom 2: The routes in BGP may not get installed to RIB.

Conditions: These symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 .... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

Workaround for symptom 1: Remove import-route target and reconfigure route-target.

Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

CSCtr91106

A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS Software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

CSCts00341

Symptoms: When executing a CLI that requires domain-name lookup such as ntp server domain.com, the command fails with the following message on the console:

ASR1k(config)#ntp server server.domain.com <<< DNS is not resolved with dual RPs on ASR1k
Translating "server.domain.com ...domain server (10.1.1.1) [OK]

%ERROR: Standby doesn't support this command
% Invalid input detected at '^' marker.

ASR1k(config)#do sh run | i ntp
ASR1k(config)^

Conditions: This symptom occurs on a redundant RP chassis operating in SSO mode.

Workaround: Instead of using hostname in the command, specify the IP address of the host.

CSCts13255

Symptoms: Standby SUP720 crash is observed on the Cisco 7600 router in c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:

%CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONITOR peer process has failed to receive heartbeats
Conditions: This symptom is observed on the Cisco 7600 router with mistral based supervisors like SUP720. This issue is fairly uncommon, but affects all the versions after Cisco IOS Release 12.2(33)SRE -- this includes 15.0S, 15.1S and 15.2S. This doesn’t affect RSP 720.

Workaround: There is no workaround.

- **CSCts23882**
  - Symptoms: ISG calculates the radius response authenticator in CoA account-profile-status-query replies wrongly, resulting in a invalid response.
  - Conditions: This symptom is observed when the CoA/WWW based session authentication is triggered via a CoA account logon using the “old” SSG command attributes.
  - Workaround: Configure a fix “NAS-IP-Address” value with the `radius-server attribute 4 x.x.x.x` command.

- **CSCts38429**
  - The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.
  - Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

- **CSCts56044**
  - Symptoms: A Cisco router crashes while executing a complex command. For example:
    - `show flow monitor access_v4_in cache aggregate ipv4 precedence sort highest ipv4 precedence top 1000`
  - Conditions: This symptom is observed while executing `show flow monitor top top-talkers` command.
  - Workaround: Do not execute complex flow monitor top-talker commands.

- **CSCts67465**
  - Symptoms: If you configure a frequency greater than the enhanced history interval or if the enhanced history interval is not a multiple of the frequency, the standby will reset.
  - Conditions: This symptom is observed always, if the standby is configured as an SSO.
  - Workaround: Remove enhanced history interval configuration before resetting the frequency.

- **CSCts70790**
  - Symptoms: A Cisco 7600 router ceases to advertise a default route configured via `neighbor default-originate` command to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.
  - Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.
  - Workaround: Remove and readd the `neighbor default-originate` command on the Cisco 7600 router and do a soft clear for the VRF neighbor.
Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

A workaround is available to mitigate this vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-rsvp

Symptoms: The following error message is displayed:

%FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi (0x104C2E4)

Conditions: This symptom is seen when clearing the sessions after a long time, and the memory leak increases incrementally. Leak is very slow.

Workaround 1: Do not bring down all sessions together.

Workaround 2: Do not tear down the sessions (scale numbers: 4k and above) together from different sources (say clearing PPP sessions and ISG sessions in lab; in field, clearing might happen via other triggers) simultaneously with no time gap between them.

Workaround 3: Do not have accounting accuracy configured.

Workaround 4: In this case, ISG Features are applied on TC and Session both. If we do not apply the features on the TCs, chances of this happening are less.

Symptoms: Active crashes upon configuring a large number of TP tunnels with scale configurations either using copy paste or loading from a configuration file.

Conditions: This symptom is not very consistent, not reproducible all the time, and happens only on adding tunnel TP configurations. The crash occurs when the protect-lsp is being configured.

Workaround: Manually add the MPLS-TP tunnels through CLI instead of copying from a configuration or copy pasting a large configuration.

Symptoms: PIM Assert is sent out from a router with metric [0/0], though the router has a less preferred path to reach the Source or RP.

Conditions: This symptom occurs when an mroute is first created and its RPF lookup to the Source or RP is via BGP or Static, which involves recursive lookup, or there is no valid path to reach Source or RP. This issue only occurs in a small window in milliseconds. After the window, the metric [0/0] is corrected.

Workaround: There is no workaround.

Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.

Conditions: This symptom is observed only with IPv6, and not with IPv4.

Workaround: Disable IPv6 CEF.
• CSCtt01056
Symptoms: When a shell map configuration includes a parameter with no default value, that is, parameter1="" or """, then that parameter should be considered mandatory. During service activation of that shell map, if parameter1 is not provided by Radius, the activation should be rejected:
  - In case of service activation from Access-Accept, the session should be terminated.
  - In case of service activation from COA, the COA should be NAKed, and the services rolled back.
Conditions: This symptom is observed with a shell map configuration when some parameters do not have the default value configured, such as param="" or """". This issue is seen with service activation with a missing mandatory parameter.
Workaround: There is no workaround.

• CSCtt02313
Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code was integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.
Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.
Workaround: There is no workaround.

• CSCtt02645
Symptoms: CPUHOG is seen due to flapping of all NHRP.
Conditions: This symptom is observed with scaling to 3k spokes on RP1.
Workaround: There is no workaround.

• CSCtt04448
Symptoms: There is a loss of IGMP snooping entries with a traffic drop at the pmLACP PoA boxes occurring.
Conditions: This symptom is observed when removing/re-adding member links.
Workaround: There is no workaround.

• CSCtt11210
Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.
The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.
Conditions: This symptom is observed when the router does not have the Root CA certificate installed.
Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

• CSCtt17785
Symptoms: In the output of show ip eigrp nei det, a Cisco ASR router reports peer version for Cisco ASA devices as 0.0/0.0. Also, the Cisco ASR router does not learn any EIGRP routes redistributed on the Cisco ASA device.
Conditions: This symptom is observed only when a Cisco ASR router is running on Cisco IOS Release 15.1(3)S and the Cisco ASA device is Cisco ASA Version 8.4(2).
Caveats in Cisco IOS XE 3.5S Releases

Workaround: Downgrade the Cisco ASR router to Cisco IOS Release 15.1(2)S.

- **CSCtt17879**
  Symptoms: The `bgp network backdoor` command does not have any effect.
  Conditions: This symptom occurs:
  - On 64-bit platform systems.
  - When the network is learned after the backdoor has been configured.
  Workaround: Unconfigure and reconfigure the network backdoor.

- **CSCtt26643**
  Symptoms: A Cisco ASR 1006 router running Cisco IOS Release 15.1(2)S2 or Cisco IOS Release 15.1(3)S0a crashes with Signal 11.
  Conditions: This symptom is observed on a Cisco ASR 1006 router running the “asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin” image. The `show version` command causes the “Last reload reason: Critical software exception” error.
  Workaround: There is no workaround.

- **CSCtt28703**
  Symptoms: VPN client with RSA-SIG can access a profile where the CA trustpoint is not anchored.
  Conditions: This symptom is observed if RSA-SIG is used.
  Workaround: Restrict access by using a certificate-map matching the right issuer.
  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.5/3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:P/I:N/A:N/E:POC/RL:W/RC:C
  No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- **CSCtt29615**
  Symptoms: Any CLI command issued under af-interface mode in EIGRP router may lead to router crash.
  Conditions: This problem is observed in a Cisco router that is running Cisco IOS Release 15.2(1)S.
  Workaround: There is no workaround.

- **CSCtt31634**
  Symptoms: Traffic drops.
  Conditions: This symptom occurs when the hw-module reloads the IM on active and posts which switchover is performed.
  Workaround: After switchover, use the `hw-module subslot reload` command to recover from the problematic state, and traffic will resume.

- **CSCtt32165**
  Symptoms: The Cisco Unified Border Element Enterprise on the Cisco ASR 1000 series router can fail a call with cause 47 immediately after the call connects.
Conditions: This symptom is observed with a sufficient call volume and a call flow that redirects many calls. The Cisco ASR router can fail to provision the forwarding plane for the new call due to a race condition where a prior call is not completely cleaned up on the forwarding plane before trying to use the same structure again.

The **show voice fpi stats** command output indicates that a failure has occurred if the last column is greater than zero. For example:

```
show voip fpi stats | include provision rsp
provision rsp          0      32790        15
```

Workaround: There is no workaround. However, Cisco IOS Release 3.4.1 is less impacted by these call failures due to a resolution of defect CSCts20058. Upgrade to Cisco IOS Release 3.4.1 until such time as this defect is resolved. In a fully redundant Cisco ASR 1006 router, you can failover the ESP slots to clear the hung entries in the forwarding plane. Other platforms will require a reload.

- CSCtt43843
  Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.
  Conditions: It is occurring with a Cisco 7200 platform loaded with the 15.2 (1.14)T0.1 image.
  Workaround: There is no workaround.

- CSCtt45536
  Symptoms: “FlowVar-Chunk malloc failed” messages are seen and this may be accompanied by slow console response.
  Conditions: This symptom is observed when a mix of IPv4 and IPv6 traffic is going through the router configured with QoS, VM, etc.
  Workaround: There is no workaround.

- CSCtt45654
  Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.
  Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.
  Workaround: There is no workaround.

- CSCtt70585
  Symptoms: IPv6 traffic is not flowing.
  Conditions: This symptom is seen with IPSec v6 tunnels.
  Workaround: There is no workaround.

- CSCtt95846
  Symptoms: Changing the encapsulation of an Ethernet service instance which is set up for local switching to default encapsulation may cause an error in setting up switching, resulting in an inability to switch packets.

```
PE1#show running-config | include local
connect local Ethernet0/0 1 Ethernet1/0 1
PE1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
PE1(config)#interface Ethernet0/0
```
Conditions: This symptom is observed if **no aaa new-model** command is configured.

Workaround: Unconfigure the local switching connection before changing the encapsulation of the service instance, then reconfigure the connection.

- **CSCtu01172**

  Symptoms: The Cisco ASR 1000 series router without an actual redundant router may crash when configured for CUBE HA based on the document “Cisco Unified Border Element High Availability (HA) on ASR platform Configuration Example.”

  Conditions: This symptom is observed with the Cisco ASR 1000 series router.

  Workaround: Remove the application configuration using the **no application redundancy** command.

- **CSCtu02286**

  Symptoms: With pim-bidir in MVPN core, MVPN traffic might not flow if a PE is also a rendezvous point (RP) for the pim-bidir in core.

  Conditions: This symptom occurs with pim-bidir in MVPN core.

  Workaround: Use non pim-bidir modes.

- **CSCtu12574**

  Symptoms: The **show buffers** command output displays:

  1. Increased missed counters on EOBC buffers.

  2. Medium buffer leak.

  ```
  Router#sh buffers
  Buffer elements:
  779 in free list (500 max allowed)
  1582067902 hits, 0 misses, 619 created
  
  Interface buffer pools:
  
  Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @ 00:01:17):
  273 in free list (64 min, 3000 max allowed)
  
  EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
  0 in free list (0 min, 2400 max allowed)
  2400 hits, 161836 fallbacks
  1200 max cache size, 129 in cache
  
  The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

  Conditions: The **show buffers old** command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

  This DDTS tracks the leak specific to IPC application 13-mgr.
From the `<CmdBold>show buffers old pack<noCmdBold> output:
0A9C4ED8: 00200000 02150000 0202080B 01000000 . .............. --> IPC Header
0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A .T.......I>M..|.
0A9C4EF8: 00520002 00000000 00000000 000000 .R............ --> ICC Header

And, if we look at the ICC header at the underscored items 00520002:

0052   (represents the class name)     ----> L3_MGR_DSS_REQUESTS
0002   (represents the request name)   ----> L3_MGR_MLS_REQ

Workaround: Reload the system.

- CSCtu18201
  Symptoms: A Cisco router crashes due to low stack with the following display:

%SYS-6-STACKLOW: Stack for process BGP Event running low, 0/6000

Conditions: This symptom occurs with a low stack.
Workaround: There is no workaround.

- CSCtu19450
  Symptoms: A system that is running Cisco IOS may reload when a large number of routes are simultaneously deleted at the same time that the inetCidrRouteTable is being walked.

Conditions: This symptom is only likely to happen when there are large numbers of interfaces and routes within the system, and when large numbers of routes are being rapidly removed, and the system is loaded, at the same time that the inetCidrRouteTable is being walked.

Routes may be deleted from the system both directly, and also indirectly for example, when a significant number of PPPoE sessions are removed.

Workaround: Avoid walking the inetCidrRouteTable while significant numbers of routes are being removed from the routing system.

- CSCtu29729
  Symptoms: An attempt to create a frame-relay sub-interface on a serial interface may result in error. The serial interface can then not be configured as a frame-relay interface.

Conditions: This symptom is observed when a serial interface is configured as a multi-link frame-relay bundle link with a subsequent attempt to change the configuration to a frame-relay interface.

Workaround: There is no workaround.

- CSCtu31340
  Symptoms: The `show sip call called-number` crashes the router.

Conditions: This symptom is observed when the call SIP state is DISCONNECT.
Workaround: There is no workaround.

- CSCtu33956
  Symptoms: The dialer with PPP encapsulation is seen when DSL is the WAN interface. L2PT does not work.

Conditions: This symptom is observed under the following conditions:
- The PPPoE dialer client needs to be configured on the physical SHDSL interface.
- The GRE tunnel destination interface should point to the dialer interface.
- The MPLS pseudowire should go over the tunnel interface.
- After the PPPoE session is set up, the GRE tunnel traffic gets dropped at the peer end of the PPPoE session.

Workarounds:
- There is no workaround.

- **CSCtu35713**
  Symptoms: IPv4 address saving: IPCP state change does not trigger session accounting update.
  Conditions: This symptom is observed under the following conditions:
  1. Enable IPv4 address saving on BRAS.
  2. Configure AAA periodic accounting using the `aaa accounting update periodic time in mins` command.
  3. Initiate IPCP negotiation from the client.
  4. After IPCP negotiation is complete, BRAS does not send an interim accounting update containing IPv4 address save VSA and the new IPv4 address assigned to the client.

Workaround: Configure AAA accounting with the `aaa accounting update newinfo periodic time in mins`.

- **CSCtu36674**
  Symptoms: Packets stop being transmitted in the output direction on L2transport local connect PVC on the ATM interface.
  Conditions: This symptom is observed when local connect is configured and a new ATM subinterface is configured on the same ATM main interface as the one with local connect PVC.

Workaround 1: Perform shut/no shut on local connect.
Workaround 2: Unconfigure/reconfigure local connect.

- **CSCtu39819**
  Symptoms: The Cisco ASR 1002 router configured as an RSVP Agent for Cisco Unified Communication Manager crashes under extended traffic.
  Conditions: This symptom is observed on a Cisco ASR 1002 router configured as an RSVP Agent for CUCM End-to-End RSVP feature. The router crashes after 45 minutes of traffic run with 150 simultaneous up MTP-RSVP sessions.

The image used is “asr1000rp1-adventerprisek9.03.04.00a.S.151-3.30a.bin”.

Workaround: There is no workaround.

- **CSCtu41137**
  Symptoms: IOSD Core@fib_table_find_exact_match is seen while unconfiguring tunnel interface.
  Conditions: The core is observed while doing unconfiguration.

Workarounds: There is no workaround.

- **CSCtu43731**
  Symptoms: On an RP1, RP switchover causes an RP reset.
  Conditions: This symptom is observed with RP switchover under the following conditions:
  - The router must be an RP1.
  - The configuration of Flexible NetFlow (FNF) or equivalent must be applied to 4000 or more interfaces. In this case of testing, 4000 DVTI interfaces were in use.
An equivalent of FNF is AVC or passive Video Monitoring. That is, those configured on a comparable number of interfaces will have the same effect.

Workaround 1: Prior to doing a controlled switchover, such as ISSU, deconfigure FNF from some interfaces to take it well under the threshold at which the issue can occur.

Workaround 2: Do not enable FNF monitoring.

- **CSCtu87383**
  
  Symptoms: CFM global configuration does not get applied to LC slots that are greater than 20 on LC OIR. This problem is specific to CPT platform where satellite box slot numbers go from 36 to 55.
  
  Conditions: This symptom occurs with satellite box OIR.
  
  Workaround: Disable and reenable CFM global configuration.

- **CSCtu89771**
  
  Symptoms: The Cisco ASR 1000 series router RP crashes while unconfiguring or removing the `no area 0 authentication ipsec spi <>` command.
  
  This behavior is not observed at the first few instances of unconfiguring the above CLI.
  
  Conditions: This symptom is observed only in automated tests where unconfiguring the authentication with the above CLI is executed multiple (approximately 3) times on the Cisco ASR 1000 series router. This leads to the RP crashes.
  
  Workaround: There is no workaround.

- **CSCtu92213**
  
  Symptoms: Console is stuck and irresponsive.
  
  Conditions: This symptom is seen when EVC with QoS is scaled, and traffic is being sent through many policy-maps with a large queue limit.
  
  Workaround: Configure a smaller queue-limit under each class on all egress policy-maps in use.

- **CSCtu92289**
  
  Symptoms: VCCV BFD on PW HE (routed pseudowire) is not working.
  
  Conditions: VCCV BFD is not working on routed pseudowire but works fine on scalable EoMPLS.
  
  Workaround: There is no workaround.

- **CSCtu92673**
  
  Symptoms: L2TP tunnels are not getting established with PPPoE relay.
  
  Conditions: This issue is seen on a Cisco 7200 router that is running Cisco IOS Interim Release 15.2(01.12)S.
  
  Workaround: There is no workaround.

- **CSCtv19529**
  
  Symptoms: Router crashes on unconfiguring the last available DHCP pool. Crash will also be seen on running the `no service dhcp`.
  
  Conditions: This crash can happen only if “DHCP Client” process is running on the router along with the DHCP relay processes (DHCPD Receive, DHCPD Timer, DHCPD Database).
  
  The client process can be started:
  
  1. from an DHCP autoinstall attempt during router startup (with no nvram config).
  2. if the `ip address dhcp` is run on one of the interfaces.
3. if the router was used for DHCP proxy client operations.

The relay processes are started when a DHCP pool is created by the `ip dhcp pool pool` command.

Workaround: Have a dummy DHCP pool created using the `ip dhcp pool dummy_pool` command, and never delete this pool. Other pools can be created and removed at will, the `dummy_pool` should not be removed. In addition, do not execute the `no service dhcp` command.

- CSCtw43640
  
  **Symptoms:** An IP ping/CFM session through Handoff FPGA fails.
  
  **Conditions:** This symptom is observed after switchover with IM in slot 5.
  
  **Workaround:** There is no workaround.

- CSCtw45055
  
  **Symptoms:** A Cisco ASR router may experience a crash in the BGP Scheduler due to a segmentation fault if BGP dynamic neighbors have been recently deleted due to link flap. For example:

  ```
  Nov 10 08:09:00.238: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
  Nov 10 08:10:20.944: %BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold time expired) x bytes
  Nov 10 08:10:20.944: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification received
  Nov 10 08:10:20.945: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from session Neighbor deleted
  Nov 10 08:10:51.816: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
  
  Exception to IOS Thread:
  Frame pointer 0x3BE784F8, PC = 0x104109AC
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler
  
  The scheduler process will attempt to reference a freed data structure, causing the system to crash.
  
  **Conditions:** This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.
  
  **Workaround:** There is no workaround.

- CSCtw45168
  
  **Symptoms:** DTMF interworking fails when MTP is used to convert OOB---RFC2833 and vice versa.
  
  **Conditions:** This symptom is observed when MTP is used to convert OOB---RFC2833 and vice versa. This issue is seen starting from Cisco IOS XE Release 3.2S. Cisco IOS XE Release 3.1S should work fine.
  
  **Workaround:** There is no workaround.

- CSCtw46625
  
  **Symptoms:** The QL value is DNU although the four least significant bits of SSM S1 byte are pointing to PRC (bits: 0010).
  
  **Conditions:** This symptom is observed when SSM S1 byte is received on CEoPs SPAs or channelized SPA-1XCHSTM1/OC3.
  
  **Workaround:** Force the QL PRC value by executing the following command:

  ```
  network-clock quality-level rx QL-PRC controller SONET 1/2/0
  ```
• CSCtw48209
Symptoms: High-end Cisco devices running Cisco IOS are likely affected. Active features at the
time of this problem manifestation include any condition that leads to RSVP SNMP notification
generation in Cisco IOS. BGP/MPLS TE instability, leading to changes to RSVP session status
change, is observed in a test scenario while running Cisco IOS Release SXI4 and Cisco IOS
Release SXI7. The issue is not reproducible consistently.
Conditions: This symptom is observed with Cisco IOS Release SXI4, Cisco IOS Release SXI7,
Workaround: Disable RSVP notification using the no snmp-server enable traps rsvp command.

• CSCtw50277
Symptoms: Policy manager is getting apply config failed on standby while policy is activated
through CoA. The router later crashes in policy code.
Conditions: This symptom is seen when CoA activated policy install is failing on standby RP.
Workaround: There is no workaround.

• CSCtw51134
Symptoms: IMA interface configuration is lost post stateful switchover (SSO).
Conditions: This symptom occurs after SSO.
Workaround: There is no workaround.

• CSCtw52504
Symptoms: WAN mode is not enabled on 10G IMs.
Conditions: This symptom is observed when a 10G IM operates in LAN mode by default. The WAN
mode supports SONET alarms to interface with SONET-like equipments.
Workaround: There is no workaround.

• CSCtw52610
Symptoms: Some of the TCes will switch to fallback interface, and the remaining TCes on primary
interface will be in OOP state.
Conditions: The issue is seen when primary link is considered OOP based on utilization despite
using the no resolve utilization command.
Workaround: There is no workaround if PfR policy with and without utilization is needed. If PfR
policy based on utilization is not needed, then configure using the max-xmit-utilization percentage
100 command.

• CSCtw58395
Symptoms: When executing the clear crypto session command in 4k FlexVPN cases, the memory
of crypto IKEv2 is increasing.
Conditions: This symptom is observed when the session is flapping.
Workaround: There is no workaround.

• CSCtw58586
Symptoms: IKEv2 CLI configuration currently requires to manually link the crypto IKEv2 profile
default to the crypto IPSec profile default. This enhancement request will change the behavior and
create an automatic anchorage.
Conditions: This symptom is seen in IKEv2 usage.
Caveats in Cisco IOS XE 3.5S Releases

Workaround: There is no workaround.

- CSCtw64040
  Symptoms: Crash due to MPLS, which appears to be associated with load-balancing.
  Conditions: This symptom occurs when MPLS is configured.
  Workaround: There is no workaround.

- CSCtw68745
  Symptoms: A Cisco ASR 1000 router acting as DHPCv6 Relay standby crashes when there is high DHCPv6 incoming traffic and if DHCPv6 relay is configured on many (around 5k) interfaces.
  Conditions: This symptom occurs when there is high DHCPv6 incoming traffic and if DHCPv6 relay is configured on many (around 5k) interfaces.
  Workaround: There is no workaround.

- CSCtw73551
  Symptoms: Standby RP can crash due to a memory leak processing calls. The crashinfo file identifies the process as follows:

  UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps

  Conditions: This symptom is seen on CUBE enterprise on the Cisco ASR 1000 series router with redundant RPs and approximately 2.4 million calls processed from last start of the standby RP.
  Workaround: There is no workaround.

- CSCtw76044
  Symptoms: Need IGMP/MLD information to make IGMP/MLP snooping work.
  Conditions: This symptom is observed under all conditions.
  Workaround: There is no workaround.

- CSCtw79579
  Symptoms: Standby fails to be in standby HOT state after reload.
  Conditions: This symptom is seen after removal of an IM and doing RSP stateful switchover (SSO) and then trying to bring up the standby RSP.
  Workaround: There is no workaround.

- CSCtw85883
  Symptoms: The error “ace_add_one_map failed” occurs while adding an ACE to a crypto acl that is being used by a crypto map.
  Conditions: This symptom is observed when the crypto map is applied to an interface and the crypto acl being modified is also in use.
  Workaround: Remove the crypto map and apply the ACL changes to avoid the error.

- CSCtw94319
  Symptoms: Crash is seen at dhcpd_forward_request.
  Conditions: This symptom is seen when the IP DHCP Relay feature is used in scaled configuration.
  Workaround: Remove the ip dhcp relay information option vpn command, if possible. Otherwise, there is no workaround.
- **CSCtw99290**
  Symptoms: The source or destination group-address gets replaced by another valid group-address.
  Conditions: This symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.
  Workaround: There is no workaround.

- **CSCtw99877**
  Symptoms: IOMD process on 10G IM crashes upon booting standby.
  Conditions: This symptom is observed when the interface state is down on active.
  Workaround: There is no workaround.

- **CSCtx01604**
  Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.
  Conditions: This problem presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.
  Workaround: Do not use any dynamic network interface IP address as CNS ID.

- **CSCtx05942**
  Symptoms: The session to the service module from the Supervisor Fails. This can happen with SAMI, NAM, NAM-2 etc. modules.
  For example, if the SAMI card is in Slot 2, the `session slot 2 proc 0` command fails to create a telnet session and fails to give out the following messages:

    SUP#session slot 2 proc 3
    The default escape character is Ctrl-^, then x.
    You can also type 'exit' at the remote prompt to end the session
    Trying 127.0.0.33 ...
    % Connection timed out; remote host not responding

  Conditions: This symptom occurs with 15.2(1)S release. It is not observed with Cisco IOS Release 15.1(3)S1 or lower version.
  Workaround: Downgrading the Supervisor to Cisco IOS Release 15.1(3)S1 or lower version resolves this issue.

- **CSCtx09614**
  Symptoms: With the preconfigured ATM configuration, the standby RSP does not boot up.
  Conditions: This symptom is observed when one of the RSPs is up and the running configuration has the ATM configuration under the controller.
  Workaround: There is no workaround. Without an ATM configuration, the standby RSP goes to standby mode.

- **CSCtx21206**
  Symptoms: BFDv6 hardware offloaded sessions do not come up with all IPv6 source addresses.
  Conditions: This symptom is observed with interface source IPv6 addresses that have some specific bits in the 6th byte set like 6001:1::C::1.
Workaround: Reconfigure the source IPv6 addresses to some address that will not match the criteria mentioned in the above Conditions.

- CSCCtx29543
Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the show ip route command.
Conditions: This symptom occurs under the following conditions:
1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exist.
2. A default route exists.
3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.
The router may now crash when doing show ip route command or when default route is updated.
Workaround: There are two possible workarounds:
1. Ensure that not all 23 supernet mask lengths are populated by doing route filtering.
2. If workaround #1 is not possible, then insure that at least one supernet route for all possible mask lengths exists at all times, for example by configuring summary routes that do not interfere with normal operation.

- CSCts29892
Symptoms: The mtu command is not allowed on BDI interfaces on the Cisco ASR 903 router.
Conditions: This symptom occurs when you configure the mtu command on BDI interfaces.
Workaround: There is no workaround. However, note that the ip mtu command is supported on BDI interfaces.

Open Caveats—Cisco IOS XE Release 3.5.0S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.5.0S.

- CSCtg68047
Symptoms: The router reloads.
Conditions: This symptom is observed if several tunnels with crypto protection are being shut down on the router console and the show crypto sessions command is executed simultaneously on another terminal connected to the router.
Workaround: Wait until the tunnels are shut down before issuing the show command.

- CSCtj58706
Symptoms: On executing ISSU runversion, the standby RP reloads multiple times before reaching hot-standby.
Conditions: This symptom is observed during ISSU upgrade/downgrade with the iso1-iso2 image. This issue is seen with scaled configuration of 7000 L2VPN, 300 BGP, 300 EIGRP, and 8000 EVC sessions.
Workaround: There is no workaround.

- CSCtk62763
Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.
Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.

Workaround: There is no workaround.

- CSCtn83900
  Symptoms: After performing legacy mode or native mode subpackage ISSU with flexible NetFlow configured, the interface to monitor bindings may not be present on the newly active RP.
  Conditions: This symptom is observed when a legacy mode or native mode subpackage ISSU is performed with FNF configured.
  Workaround: Remove the FNF monitors prior to the subpackage ISSU. Add the monitors back to the interface configuration after the upgrade. Alternatively, use super-package ISSU, which does not have this limitation.

- CSCto71671
  Symptoms: Using the radius-server source-ports extended command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.
  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.
  Workaround: There is no workaround.

- CSCtq80891
  Symptoms: The Processor Pool for the Cisco IOS memory is used up with most of the buffers in the “IPv6 PIM input queue”.
  Conditions: This symptom is observed with the following topology:
  - 500 IPv6 Sources sending Mcast traffic to 500 IPv6 Mcast groups
  - 500 PIM-RP on UUT
  - 500 PIM-RP Acl to make sure 1 Mcast-group/Tunnel
  - The GRE tunnels could be configured with tunnel protection or not.
  The reproduce procedure is as follows:
  1. Copy configurations (IPv6 over IPv4 GRE Tunnel Protections and IPv6 Mcast included) to TR1, TR2, and UUT.
  2. Launch Mcast traffic (500M) on IXIA.
  3. Hit the Cisco IOS memory depletion issue on UUT.
  Workaround: Configure the punt policer for PIM register packets as follows:
  platform punt-policer 55 limit-number
  platform punt-policer 55 limit-number high
  The limit-number above is a number between 1000-2000.

- CSCtr80274
  Symptoms: CISCO-LICENSE-MGMT-MIB does not populate.
Conditions: This symptom occurs when the required license is installed on the Cisco ASR 903 router, but the SNMP query does not return any value.

```
ASR903#show license
Index 1 Feature: metroaggrservices
  Period left: Life time
  License Type: Permanent
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Medium
Index 2 Feature: metroipservices
  Period left: 8 weeks 4 days
  License Type: Evaluation
  License State: Active, Not in Use, EULA not accepted
  License Count: Non-Counted
  License Priority: None
Index 3 Feature: metroservices
  Period left: 8 weeks 4 days
  License Type: Evaluation
  License State: Active, Not in Use, EULA not accepted
  License Count: Non-Counted
  License Priority: None
```

Workaround: There is no workaround.

- **CSCts05124**

  Symptoms: A zero-byte crash file is generated upon a crash with TREX SPA.

  Conditions: This symptom is observed with a test crash on a SIP-400 line card with TREX SPA inserted.

  Workaround: There is no workaround.

- **CSCts11715**

  Symptoms: After shutting the tunnel, ISAKMP does not turn OFF.

  Conditions: This symptom is observed in a scaled DMVPN setup with more than 1k spokes.

  Workaround: There is no workaround.

- **CSCts12499**

  Symptoms: SPA firmware crash at one bay leads to SPA crash in another bay.

  Conditions: This symptom is observed when “test crash cema” is executed from the SPA console. leading to the SPA in the other bay to reload. Also, the crashinfo is not present in the RP disk.

  Workaround: There is no workaround.

- **CSCts13255**

  Symptoms: Standby SUP crash is observed on the Cisco 7609 router after upgrade to c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:
%CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONIT or peer process has failed to receive heartbeats

Conditions: This symptom is observed on the Cisco 7609 router after upgrade to c7600s72033-adviceervicesk9-mz.150-1.S3a.bin. This issue is also seen with Cisco IOS Release 12.2(33)SRE.

Workaroud: There is no workaround.

- CSCts47550
  Symptoms: When applying protocol attributes policy rules, traceback may be seen.
  Conditions: This symptom is not consistent and may or may not appear when applying the protocol attributes policy rules. This symptom is also not consistent with a specific protocol, but may appear with respect to different protocols.
  Workaroud: There is no workaround.

- CSCts63426
  Symptoms: With 1K EoMPLS PWs, 6 percent performance drop is observed in Cisco IOS XE Release 3.5 compared to Cisco IOS XE Release 3.4 performance.
  Conditions: This symptom is observed with 1K EoMPLS PWs in Cisco IOS XE Release 3.5.
  Workaroud: There is no workaround.

- CSCts63658
  Symptoms: Multicast traffic do not flow over EVCs on the port-channel.
  Conditions: This symptom is observed during router reload.
  Workaroud: Reconfigure after the router reload. Configure regular EFPs before EFPs on the PC in the same BD.

- CSCts82598
  Symptoms: Incorrect IP from the NAT pool is chosen for translation, when one protocol exhausts all ports of all IPs and another protocol traffic is received.
  Conditions: This symptom occurs when one protocol (for example, TCP) exhausts all ports of all IPs in a pool, and only one IP from the pool is selected for translation, thus limiting the capacity of creating translations. This happens only when one protocol completely exhausts all ports and then another protocol traffic starts. This usually is not the case in customer environments that mostly see both TCP and UDP traffic hitting the box time.
  Workaroud: There is no workaround.

- CSCts97925
  Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.
  Conditions: This symptom is observed only with IPv6, and not with IPv4.
  Workaroud: Disable IPv6 CEF.

- CSCtt01056
  Symptoms: When a shell map configuration includes a parameter with no default value, that is, parameter1="", "<>", or ", then that parameter should be considered mandatory. During service activation of that shell map, if parameter1 is not provided by Radius, the activation should be rejected:
  - In case of service activation from Access-Accept, the session should be terminated.
  - In case of service activation from COA, the COA should be NAKed, and the services rolled back.
Conditions: This symptom is observed with a shell map configuration when some parameters do not have the default value configured, such as param="", "<>", or "". This issue is seen with service activation with a missing mandatory parameter.

Workarounds:

- **CSCt02645**
  Symptoms: CPUHOG is seen due to flapping of all NHRP.
  Conditions: This symptom is observed with scaling to 3k spokes on RP1.
  Workaround: There is no workaround.

- **CSCt04724**
  Symptoms: On PPPoEoX, when activating multiple services from Access-Accept with long Cisco-SSG-Account-Info strings, if the aggregated string length exceeds the current limit of 256 characters, then the service activation fails, a traceback is seen, and the session is allowed to establish, no services will be applied in the ingress and/or egress directions.
  Conditions: This symptom is observed when the aggregated services string length exceeds the limit (256 characters).
  Workaround: The session should be terminated instead. In case of service activation from CoA, if the cumulative services string length exceeds the limit, then the last CoA should be NAKed, and the services rolled back to the previous state.

- **CSCt11210**
  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.
  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.
  Conditions: This symptom is observed when the router does not have the Root CA certificate installed.
  Workarounds: Install the Root CA certificate in a separate trustpoint on all involved routers.

- **CSCt11558**
  Symptoms: The Cisco ASR 1000 router displays the “INVALID_GPM_ACCESS” error message due to invalid GPM load. This may cause unexpected Embedded Services Processors (ESP) reload.
  Conditions: This symptom is observed when a small packet is sent from a BDI interface to an Ethernet service instance with either the **rewrite egress tag** command or the **rewrite ingress tag** command with the symmetric option present.
  Workarounds: There is no workaround.

- **CSCt21257**
  Symptoms: After a reload or switchover, all interfaces on one or more IMs may be down down. The state of the IMs is “ok, active”, which is shown in the show platform command output.
  Conditions: This symptom is occasionally observed after a reload or a switchover.
  Workarounds: Power cycle the box.

- **CSCt26532**
  Symptoms: With QoS policy-map configured on a BFD interface, modifying the QoS policy-map flaps the BFD session.
  Conditions: This symptom is observed when BFD and QoS policy-maps are configured on the same interface.
Workaround: There is no workaround.

Further Problem Description: QoS and BFD use a common flag that gets reset and set during QoS policy-map update, causing the BFD session to flap. BFD session flap leads to the OSPF session also going down.

- CSCtt33937

Symptoms: Configure port 7 on the Gigabit IM as a port to forward traffic using IP routing.

```
config t
interface g0/0/7
ip address 10.0.0.1 255.255.255.0
```

Conditions: This symptom is observed when traffic is flowing well. When you perform a switchover, and once the standby becomes the new active, the traffic does not hit the ingress counter of the interface itself. On checking the links status using the registers, the SGMI link appears out of sync.

Workaround: There is no workaround. Reload the box when this symptom is observed.

- CSCtt34361

Symptoms: During a soak test with 1800 PPPoE sessions flapping with the IPv4 Saving feature enabled + per-user ACLv4 and ACLv6, there is no ISG service. After 56 iterations, one memory snapshot is taken every four iterations, that is, roughly 270 seconds per iteration. The test duration is 4 hours, with total 100800 sessions established with an average of 7cps.

Conditions: This symptom occurs under the following conditions:

1. No active session is there in the router.
2. Establish 1800 PTA dual-stack sessions with per-user ACL from Radius + IPV4 Saving feature.
3. Wait till all sessions come UP.
4. Take a memory leak snapshot “high”.
5. Wait for all sessions to time out on the Idle timer (no traffic).
6. Wait for all sessions to go DOWN.
7. Take a memory snapshot.
8. Loop back to 1.

Workaround: There is no workaround.

- CSCtt45654

Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

Workaround: There is no workaround.

- CSCtt45801

Symptoms: The DMVPN HUB RP crashes with the default EIGRP timer when scaling to 4k spokes.

Conditions: This symptom occurs when scaling to 4k spokes.

Workaround: Changing the EIGRP timer to longer may reduce the chances of a crash.

- CSCtt70133

Symptoms: The RP resets with FlexVPN configuration.
Conditions: This symptom is observed when using the clear crypto session command on the console.
Workarounds: There is no workaround.

- **CSCtt70346**
  Symptoms: IOMD crash is seen when running the PTP session.
  Conditions: This symptom is observed when running the PTP session for a long time. Sometimes, this issue is seen when changing PTP packet rates. This issue is seen rarely.
  Workarounds: There is no workaround.

- **CSCtt70498**
  Symptoms: After a reload or switchover, the state of F0 or F1 may become “disconnecting” instead of “ok, active/standby”, which is shown in the show platform command output. As a result, the corresponding RSP does not forward traffic.
  Conditions: This symptom is occasionally observed after a reload or a switchover.
  Workarounds: Power cycle the box.

- **CSCtt94147**
  Symptoms: Nile manager crash is observed.
  Conditions: This symptom is observed with the following conditions:
  - VPLS in the core.
  - REP in the access.
  - The access-side REP segment flaps a few times.
  Workarounds: There is no workaround.

- **CSCtt94566**
  Symptoms: The router crashes before all sessions come up.
  Conditions: This symptom occurs before all sessions come up.
  Workarounds: There is no workaround.

- **CSCtt95577**
  Symptoms: After creating the 994th VC on a T1/E1 IM on the Cisco ASR 903 router, the traffic flow stops. Packets get dropped on the egress on the router.
  Conditions: This symptom is observed when ping starts to fail on all the pre-existing VCs upon adding the 994th VC. The working is unaffected till 993 VCs.
  Workarounds: Delete the 994th VC to make the pre-existing VCs forward traffic.

- **CSCtt97164**
  Symptoms: If the router interface is flapped, the HSRP message may be dropped by the punt/inject path.
  Conditions: This symptom is seen if the router interface is flapped.
  Workarounds: Disable the inject bypass.

- **CSCtt97473**
  Symptoms: After a reload or switchover, the RSP may reset during bootup.
  Conditions: This symptom is observed occasionally after a reload or switchover.
  Workarounds: There is no workaround.
- **CSCtt98574**
  Symptoms: After a reload or switchover, the state of one or more IMs may become “out of service” instead of “ok, active/standby”, which is shown in the `show platform` command output. As a result, the corresponding interfaces do not come up.
  Conditions: This symptom is occasionally observed after a reload or a switchover.
  Workaround: Power cycle the box.

- **CSCtt99235**
  Symptoms: After a switchover, an IOMD process crashes because it has failed to establish LIPC connection.
  Conditions: This symptom is seen occasionally after a switchover.
  Workaround: Reload the box.

- **CSCtu02280**
  Symptoms: When running the PTP session for an extended period of time, there is a very small likelihood of PTP daemon crashing.
  Conditions: This symptom occurs when running the PTP session for a long time.
  Workaround: There is no workaround.

- **CSCtu02476**
  Symptoms: An SSO followed by a change in the xconnect MTU results in the pseudowire in the redundant RP to go down. The pseudowire in the Active RP remains up and running. A subsequent SSO results in the pseudowire to go down.
  Conditions: This symptom is observed with “encapsulation default” at that end of the pseudowire where SSO is performed. An SSO followed by a change in the MTU value, and then a subsequent SSO, causes the pseudowire to go down. This issue is also seen in a setup with redundant pseudowires, where the primary and backup pseudowires configured under the service instance do not come up after changing the MTU with SSO.
  Workaround: Execute “no xconnect” under the service instance, and then reconfigure the pseudowire with the new MTU value under the service instance.

- **CSCtu03699**
  Symptoms: The Nile Manager crashes.
  Conditions: This symptom is observed when reloading the TP tunnel endpoint multiple times.
  Workaround: There is no workaround.

- **CSCtu12574**
  Symptoms: The `show buffers` command output displays:
  1. Increased missed counters on EOBC buffers.
  2. Medium buffer leak.

  ```
  Router#sh buffers
  Buffer elements:
    779 in free list (500 max allowed)
    1582067902 hits, 0 misses, 619 created
  Interface buffer pools:
    ....
  Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647)
  ```
The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

Conditions: The show buffers old command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

The DDTS CSCtr34960 tracks the leak specific to IPC application l3-mgr.

From the show buffers old pack output:

And, if we look at the ICC header at the underscored items 00520002:

Workaround: Reload the system.

- CSCtu13806
  Symptoms: Upon switchover, the “red_switchover_process” process causes a crash on the old active RSP.
  Conditions: This symptom is observed upon switchover.
  Workaround: This crash is harmless as another RSP becomes active and works properly. Reboot the RSP to make it come up as standby.

- CSCtu13951
  Symptoms: Pending objects appear on the active and standby ESP.
  Conditions: This symptom occurs when the edge device to the core link is flapped multiple times for close to two days.
  Workaround: There is no workaround.

- CSCtu17006
  Symptoms: Mediatrace is not working because RSVP fails to select the output interface.
  Conditions: This symptom is observed only with PFR configuration.
  Workaround: Remove the PFR configuration.

- CSCtu17296
  Symptoms: Traffic failure occurs on 3 to 4 VLANs out of 1000.
  Conditions: This symptom is observed after reloading the UUT.
Caveats in Cisco IOS XE 3.5S Releases

- **CSCtu17540**
  Symptoms: IOMD core is generated on switchover for T1/E1 IM. After switchover, the IOMD process is aborted.
  Conditions: This symptom is observed with every switchover.
  Workaround: There is no workaround.

- **CSCtu18150**
  Symptoms: FP crash occurs due to a wrong FCID handling issue.
  Conditions: This symptom occurs due to a wrong FCID handling issue.
  Workaround: There is no workaround.

- **CSCtu24765**
  Symptoms: Under scale (28.8K PPPoX sessions), when executing “show policy-map session” from the CLI, both ESPs crash.
  Conditions: This symptom is observed with a large scale, that is, 28K PPPoE sessions established + ISG QoS services.
  Workaround: There is no workaround.

- **CSCtu27601**
  Symptoms: On ATM BRAS under scale (16K PPPoEOA sessions + ISG services), the ESP crashes occasionally during sessions establishment.
  Conditions: This symptom is observed with a large scale (16K PPPoEOA sessions + services).
  Workaround: There is no workaround.

- **CSCtu28990**
  Symptoms: RP crash is observed at SYS-6-STACKLOW: Stack for process XDR Mcast.
  Conditions: This symptom is observed when performing shut/no shut on interfaces on a configuration-rich system.
  Workaround: There is no workaround.

- **CSCtu29047**
  Symptoms: After a reload or switchover, the RSP may exhibit a kernel hang.
  Conditions: This symptom is observed occasionally after a reload or switchover.
  Workaround: Power cycle the box.

- **CSCtu32935**
  Symptoms: IPv6 traffic loss of around 30 seconds is seen for routes learned from dynamic routing protocols upon RSP switchover with the Nonstop Forwarding (NSF) configuration. IPv6 CEF is not programmed on the standby RSP.
  Conditions: This symptom is observed with RSP switchover.
  Workaround: There is no workaround for the dynamic routing protocol. Problem will not be seen for static route.

- **CSCtu33258**
  Symptoms: LDP over MPLS-TP tunnel fails to get established upon router reload.
Conditions: This symptom is seldom seen when the router is reloaded with scaled MPLS-TP tunnels that have LDP session established over the tunnels. Pinging traffic through the tunnel fails.

Workarounds:

- **CSCtu34906**
  Symptoms: All ptp sessions go down on the BC upon configuring more than 63 slaves to negotiate with it.
  Conditions: This symptom is observed on the BC when there are more than 63 slaves trying to negotiate with the master. This issue is not seen with lesser number of slaves. It was verified that the sessions are stable with 62 slaves. This issue is also not seen with the OC master, but only with the BC master.
  Workarounds: This issue is not seen with lesser number of slaves. It was verified that the sessions are stable with 62 slaves. This issue is also not seen with the OC master.

- **CSCtu35713**
  Symptoms: IPv4 address saving: IPCP state change does not trigger session accounting update.
  Conditions: This symptom is observed under the following conditions:
  1. Enable IPv4 address saving on BRAS.
  2. Configure AAA periodic accounting using the `aaa accounting update periodic time in mins` command.
  3. Initiate IPCP negotiation from the client.
  4. After IPCP negotiation is complete, BRAS does not send an interim accounting update containing IPv4 address save VSA and the new IPv4 address assigned to the client.
  Workarounds: Configure AAA accounting with the `aaa accounting update newinfo periodic time in mins` command.

- **CSCtu41497**
  Symptoms: The Nile Manager crashes.
  Conditions: This symptom is observed with a 256 rmep scale.
  Workarounds: There is no workaround.

- **CSCtu43120**
  Symptoms: Service accounting start is not sent for L2TP sessions.
  Conditions: This symptom is observed with L2TP.
  Workarounds: There is no workaround.

- **CSCtv22685**
  Symptoms: The ESP on the Cisco ASR 1000 router crashes or the GRE tunnel does not switch over when the destination interface is removed or the route changes, causing the tunnel interface to stop forwarding packets.
  Conditions: This symptom is observed when multiple GRE tunnels are configured on the same interface(s) with a high traffic rate across the tunnels.
  Workarounds: Only configure one GRE tunnel per physical interface.

- **CSCtu98727**
  Symptoms: ANCP shaping with Model F fails with BRR classes.
Conditions: This symptom is observed with BRR classes, but works fine with LLQ (priority level) classes.

Workaround: There is no workaround.

- CSCtv14686
  Symptoms: When a hierarchical policy with more than one VLAN class uses the same child policy, such an HQoS policy will not work and the support will be tracked via CSCtw44894.
  Conditions: This symptom is observed when a hierarchical policy with more than one VLAN class uses the same child policy.
  Workaround: Ensure that there is a different child policy-map attached to each VLAN class. The child policy-maps could have the same content, but needs to have different policy-map names.

- CSCtr84641
  Symptoms: The misclassification issue occurs when using deny statements in the ACL for a class-map. If the packets match the deny statements, they may be not classified properly.
  Conditions: This symptom occurs when you configure deny statements in the ACL for a class-map.
  Workaround: There is no workaround.

- CSCts33401
  Symptoms: When the Cisco ASR 903 router has multiple heterogeneous ECMP paths for routing a MPLS packet to the destination, for example, one path through MPLS routing and the other through IP routing, if the IP path comes before the MPLS path in the load balance object, the Cisco ASR 903 fails to forward the MPLS packet in the hardware. The MPLS packet is either dropped or punted to Cisco IOS for routing. If the MPLS path comes before the IP path in the load balance object, MPLS packets are forwarded by the Cisco ASR 903 hardware.
  In addition, there is no issue if the incoming packet is an IP packet, even though there are multiple heterogeneous ECMP paths to reach the destination. The same issue also exists in the Whales platform for routing MPLS packets when there are multiple heterogeneous ECMP paths to reach the destination.
  Conditions: This symptom is observed with heterogeneous ECMP paths for routing an MPLS packet to the destination.
  Workaround: There is no workaround.

- CSCto58710
  Symptoms: Certificate validation fails when the CRL is not retrieved.
  Conditions: This symptom is observed when a Cisco ASR 1000 series router attempts to retrieve a CRL using LDAP, and the LDAP server is in a VRF.
  Workaround: Use a certificate map to revoke certificates or publish the CRL to an HTTP server and configure “CDP override” to fetch the CRL.
Caveats in Cisco IOS XE 3.4S Releases

This chapter provides information about caveats in Cisco IOS XE 3.4S releases. Because Cisco IOS XE 3S is based on Cisco IOS XE 2 inherited releases, some caveats that apply to Cisco IOS XE 2 releases also apply to Cisco IOS XE 3S. For a list of the software caveats that apply to Cisco IOS XE 2, see the “Caveats for Cisco IOS XE Release 2” section at the following location:

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

This chapter contains the following sections:

- Caveats in Cisco IOS XE 3.4S Releases, page 243

Caveats in Cisco IOS XE 3.4S Releases

Caveats describe unexpected behavior. 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 this chapter.

This section describes caveats in Cisco IOS XE 3.4S releases.

In this section, the following information is provided for each caveat:

- **Symptom**—A description of what is observed when the caveat occurs.
- **Conditions**—The conditions under which the caveat has been known to occur.
- **Workaround**—Solutions, if available, to counteract the caveat.

---

**Note**

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)
Resolved Caveats—Cisco IOS XE Release 3.4.6S

- CSCtj24692
  - Symptom: NVRAM configuration file gets corrupted when a chassis is power cycled without a graceful shutdown.
  - Conditions: This symptom is observed when you power cycle an ASR chassis without graceful shutdown.
  - Workaround: Shutdown chassis using “reload” command and make sure RP gets to rommon mode before power cycling the chassis.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.5S

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.4S

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.3S

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.2S

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.1S

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.0aS

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.0S

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.0S

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.0S

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.0S

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.0S

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.0S

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCtj24692
  - Symptom: CSCtj24692

Resolved Caveats—Cisco IOS XE Release 3.4.0S

- CSCtr88785
  - Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.
  - Conditions: This symptom is observed on a Cisco 3845 running the c3845-advp-servicesk9-mz.151-4. M1 image with a PKI certificate server configuration.
  - Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.
Conditions: This has been seen on Cisco IOS Release 15.1M and Cisco IOS Release 15.2T. The crash only occurs on devices that have at least one point-to-point GRE Tunnel interface configured with NHRP enabled. This type of interface is typically used to interconnect DMVPN hubs with point-to-point extension links.

Workaround: Reconfigure the point-to-point GRE extension tunnel as an mGRE interface:
- shutdown
- no tunnel destination
- tunnel mode gre multipoint
- no shutdown

The Tunnel interface must also have a static NHRP entry for the DMVPN peer, of the form:
```
 ip nhrp map remote-tunnel-address remote-NBMA-address
```
where remote-NBMA-address is the same address that was configured in the “tunnel destination” statement. On an extension link, this configuration should typically already be present.

- CSCty31407
Symptom: Netsync configuration for E1 (option 1) is not working.
Conditions: When you configure R0 as netsync source, the netsync source does not lock (only option 1), but option 2 works fine.
Workaround: There is no workaround.

- CSCty51453
Symptoms: Certificate validation using OCSP may fail, with OCSP server returning an “HTTP 400 - Bad Request” error.
Conditions: The symptom is observed with Cisco IOS Release 15.2(1)T2 and later.
Workaround 1: Add the following commands to change the TCP segmentation on the router:
```
 router(config)# ip tcp mss 1400
 router(config)# ip tcp path-mtu-discovery
```
Workaround 2: Use a different validation method (CRL) when possible.

- CSCuc42083
Symptom: fman_fp core file is seen.
Conditions: This symptom is observed when you configure GreoIPsec with tunnel protection and configure more than 1000 route-maps.
Workaround: There is no Workaround.

- CSCud44854
Symptom: Hash table is not cleared for ALG during initialization.
Conditions: This symptom is observed under the following conditions:
1. Start sip/h323/... traffic
2. Established NAT session over 60~70K
3. Send cli combinations with below actions:
   - clear ip nat trans *
   - shutdown inside / outside traffic interfaces
   - remove nat/alg config
   - reconfig nat/alg and unshut interfaces
Caveats in Cisco IOS XE 3.4S Releases

Workaround: There is no workaround.

- CSCud49494
Symptom: ESP crashed with multicast service reflection configuration when receiving UDP fragmented packets.
Conditions: This symptom is observed when multicast service reflection configured and UDP fragments is received on the VIF interface.
Workaround: There is no workaround.

- CSCud66955
Symptom: ESP crashed with multicast service reflection configuration when receiving UDP fragmented packets.
Conditions: This symptom is observed when multicast service reflection configured and UDP fragments is received on the VIF interface.
Workaround: There is no workaround.

- CSCue32352
Symptom: The aggregation-type prefix-length of PfR can not be configured less then 16. If so, the number of learned prefix will be much less then it should be.
Conditions: This symptom is observed when PfR is enabled.
Workaround: The aggregation-type prefix-length of PfR is better to be configured bigger then 24.

- CSCuf20409
Symptom: Netsync: Customer seeing clock in ql-failed state on one Cisco ASR 2RU model.
Conditions: The issue seen when distributing stratum 1 clock source through its network.
Workaround: There is no workaround.

- CSCug56942
Symptom: CUOM could not process “MOSCQEReachedMajorThreshold clear trap” from CUBE SP. For MOSCqe alert clear trap, CUBE should not sent “CurrentLevel Varbind” but should send “csbQOSAlertCurrentValue Varbind”.
Conditions: This symptom is observed when CUBE SP generates clear trap for voice quality alerts.
Workaround: The code fix is included in CUBE Cisco IOS Release 15.2(4)S4. Manually clean the alarm at CUOM after root cause is rectified if earlier CUBE version is used.

- CSCug59930
Symptom: RP and other FRUs go down and get stuck in disabled state on a 13RU-chassis. This issue is so far seen only on Cisco IOS XE 3.4 throttle branch. Cisco IOS XE 3.5 onwards has not seen this issue.
Conditions: This issue is caused by stuck midplane-lock acquired but not freed. There is a field notice about defective power supplies on Cisco ASR 1013 chassis. Please use following link and power supply module serial number to check if the power supply modules are affected.
There is a possibility of defective power supplies causing/exposing above issue.
Workaround: There is no workaround.

- **CSCug88265**
  Symptom: Looking at the output of “show platform software process list r0 sort memory”, the memory of “fman_rp” keeps increasing.
  Conditions: This symptom is observed when this box is configured as PfR border router and enabled.
  Workaround: There is no workaround.

- **CSCug98820**
  Symptom: Multicast RP-Announcement/RP-Advertisement packet is replicated more than one copy per incoming packet. The number of copies is equal to the number of interfaces/IOitems with IC flag enabled (show ip mfib to get the number of IC interfaces).
  Conditions: This symptom is observed when AUTO-RP filter is configured on PIM interfaces.
  Workaround: There is no workaround.

- **CSCuh38488**
  Symptom: An ASR with zone-based firewall enabled may drop SIP INVITE packets with the following drop reason:
  
  ```
  Router#show plat hardware qfp active feature firewall drop
  ----------------------------------------------------------------------------- Drop
  Reason Packets
  ----------------------------------------------------------------------------- L7
  inspection returns drop 1 Router#
  ```
  Conditions: This symptom is observed when the application (L7) inspection for SIP is be enabled for the flow.
  Workaround: Any of the following workarounds are applicable:
  1) Disable the port-to-application mapping for SIP with the `no ip port-map sip port udp 5060` command. This prevents ZBF from treating UDP/5060 as SIP. Instead, it is treated as simple UDP.
  2) Use the “pass” action in both directions instead of “inspect”. This disables all inspection (even L4) for the traffic.

**Resolved Caveats—Cisco IOS XE Release 3.4.5S**

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.5S.

- **CSCtl01184**
  Symptoms: Sometimes, an EVC that is configured on ES+ sends frames out with CFI bit set in the VLAN tag.
  Conditions: This symptom is observed on EVCs that are configured on ES+.
  Workaroud: There is no workaround.

- **CSCtr47317**
  Symptoms: After a switchover, a Cisco Catalyst 6500 series switch may be replicating some spanned traffic indefinitely and flooding the network with the span copies.
  Conditions: This symptom is observed after the following sequence:
  
  - An internal service module session for a FWSM or other service modules exists:

    ```
    UUT#show monitor session all
    ```
Session 1
Type: Service Module Session

- If you attempt to configure a span session with the session number already in use:
  
  UUT(config)#monitor session 1 source interface Gi2/7, Gi2/40
  
  % Session 1 used by service module

- The command seems to be rejected, but it is synchronized to the standby supervisor.

- A switchover happens.

Workaround: There is no workaround.

- CSCts40043
Symptoms: A Cisco router may crash due to a segmentation fault.

Conditions: This symptom is observed when a fail-close ACL is applied to the Gdoi crypto map in GETVPN implementation.

Workaround: There is no workaround.

- CSCts72911
Symptoms: In case of a GR/NSF peering, after an SSO, the restarting router (PE, in this case) does not advertise RT constrain filters to the nonrestarting peer (RR, in this case).

Conditions: This symptom is observed after an SSO in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the nonrestarting router does not send back the corresponding VPN prefixes towards the restarted router.

Workaround: There is no workaround.

- CSCtt35379

Conditions: This symptom can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

Workaround: Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

Note: The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes 9 Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2012 bundled publication.

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


PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9:

CVE ID CVE-2012-4617 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- **CSCtt70133**
  Symptoms: The RP resets with FlexVPN configuration.
  Conditions: This symptom is observed when using the `clear crypto session` command on the console.
  Workaround: There is no workaround.

- **CSCtt94440**
  Symptoms: The Cisco ASR 1000 series router RP may reload.
  Conditions: This symptom is observed when an etoken is in use and the `show crypto eli all` command is issued.
  Workaround: Avoid using the `show crypto eli all` command. However, you can use the `show crypto eli` command.

- **CSCtt99627**
  Symptoms: The `lacp rate` and `lacp port priority` commands may disappear following a switchover from active to standby RP.
  Conditions: This symptom affects the Cisco 7600 platform.
  Before performing a switchover one may check the configuration on the standby RP to see if the commands are present or not. If the commands are not present on the standby RP, then they will disappear if a switchover occurs.
  Workaround: Prior to switchover, if the commands do not show up on the standby RP as described above, then unconfiguring and reconfiguring the command on the active RP will fix the issue. Otherwise, if the commands disappear after a switchover, then the commands must be reconfigured on the newly active RP.

- **CSCtu22167**
  Symptoms: SP crashes.
  Conditions: This symptom is observed under the following conditions:
  - When unicast prefixes have local labels.
  - When the tunnel is the next-hop for those prefixes.
  - When the topology is modified (that is, when you remove or shut down the physical interface) so that the tunnel’s destination address is reachable via the tunnel.
  Workaround: Ensure that the tunnel endpoint peer does not advertise the prefixes to reach the tunnel endpoint.

- **CSCtu32301**
  Symptoms: Memory leak may be seen.
  Conditions: This is seen when running large `show` commands like `show tech-support` on the linecard via the RP console.
  Workaround: Do not run the show commands frequently.

- **CSCtu40028**
  Symptoms: The SCHED process crashes.
Conditions: This symptom occurs after initiating TFTP copy.
Workaround: There is no workaround.

- **CSCtu43120**
  Symptoms: Service accounting start is not sent for L2TP sessions.
  Conditions: This symptom is observed with L2TP.
  Workaround: There is no workaround.

- **CSCtw46061**
  Symptoms: The following output shows the leaked SA object continuing to be in the “OBJECT_IN_USE” state. The state is supposed to be changed to OBJECT_FREEING by crypto_engine_delete_ipsec_sa(). This is in turn being called by ident_free_outbound_sa_list().

```plaintext
shmcp-fp40#sh crypto eli
Hardware Encryption : ACTIVE
Number of hardware crypto engines = 1

CryptoEngine IOSXE-ESP(14) details: state = Active
Capability : DES, 3DES, AES, RSA, IPv6, GDOI, FAILCLOSE
IKE-Session :     0 active, 12287 max, 0 failed
DH            :   211 active, 12287 max, 0 failed
IPSec-Session :   323 active, 32766 max, 0 failed
```

Conditions: This symptom is observed on a Cisco ASR 1000 series router.
Workaround: There is no workaround.

- **CSCtw46229**
  Symptoms: Small buffer leak. The PPP LCP configuration requests are not freed.
  Conditions: This symptom is observed with PPP negotiations and the session involving PPPoA.
  Workaround: Ensure that all your PPP connections stay stable.

- **CSCtw61192**
  Symptoms: The cells keyword is added to “random-detect” whenever a policy-map is removed from an interface/map-class via “no service-policy”.
  Conditions: This symptom is observed when removing the policy-map from map-class.
  Workaround: There is no workaround.

  Further Problem Description: The CLI is technically valid if it has been manually configured as “cells” prior to the removal. The issue is that the template policy is being changed automatically to “cells” whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- **CSCtw78451**
  Symptoms: A Cisco ASR 1000 series router may reload when multiple users are logged in running show commands.
Conditions: This symptom is only seen when the Cisco ASR router is used as a DMVPN headend and there are hundreds of tunnels flapping.
Workaround: There is no workaround. However, this appears to be a timing issue when there is instability in a large-scale environment.

- CSCtw80678
Symptoms: Multilink PPP ping fails when the serial interfaces experience QMOVESTUCK error.
Conditions: This symptom may be observed if multilink PPP member links and serial interfaces on which the QMOVESTUCK error is reported are on the same SPA.
Workaround: “no shut” the interface with the QMOVESTUCK error message, remove QoS policies on the interface and subinterfaces, and remove the interface from the T1/T3 controller. Then, rebuild the configuration.

- CSCtw95466
Symptoms: When a large number of Ethernet or VLAN xconnect sessions are configured on a Cisco 7600 router, the Supervisor Processor may reload.
Conditions: This symptom is observed when aaa new-model is configured.
Workaround: Configure no aaa new-model.

- CSCtw99989
Symptoms: During normal operation a Cisco ASR 1000 Series Aggregation Services router may show the following traceback:
%FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi
Conditions: This symptom is observed during PPP renegotiation.
Workaround: There is no workaround.

- CSCtw99991
Symptoms: Chunk memory leak is seen in the ES+ LC after configuring the IP source guard EVC configurations.
Conditions: This symptom is observed on a Cisco 7600 router with ES+ LC running Cisco IOS interim Release 15.2(01.16)S.
Workaround: There is no workaround.

- CSCtx02522
Symptoms: The router displays intermittent traceback errors.
Conditions: This symptom occurs when you configure REP.
Workaround: There is no workaround.

- CSCtx04709
Symptoms: Some EIGRP routes may not be removed from the routing table after a route is lost. The route is seen as “active” in the EIGRP topology table, and the active timer is “never”.
Conditions: This symptom is seen when multiple routes go down at the same time, and a query arrives from the neighbor router. Finally, the neighbor detects SIA for the affected router and the neighbor state is flap. However, the active entry is remaining after that, and the route is not updated.
Workaround: The clear ip eigrp topology network mask command may remove an unexpected active entry.
• CSCtx11740
Symptoms: The traffic convergence takes longer because of additional/unwanted traffic is punted to CPU as we do not have *.GM code changes. The *.GM entries help drop the traffic that is not needed by MFIB (PI) code.
Conditions: This symptom is observed with link and node failures in dual-home scenarios.
Workaround: There is no workaround.

• CSCtx15650
Symptoms: PFR dynamic route-map Cisco IOS is not downloaded to hardware on the Cisco ASR 1000 or the dynamic route-map is present; however, the route-map sequences are not processed in sequential order.
Conditions: This symptom is observed with the Cisco ASR 1000 platform.
Workaround: There is no workaround.

• CSCtx32329
Symptoms: When using the `show ipv6 rpf` command, the router crashes or displays garbage for RPF idb/nbr.
Conditions: This symptom can happen when the RPF lookup terminates with a static multicast route that cannot be resolved.
Workaround: Do not use static multicast routes, or make sure that the next-hop specified can always be resolved. Do not use the `show` command.

• CSCtx35064
Symptoms: Traffic remains on a blackholed path until the holddown timer expires for a PfR monitored traffic class. Unreachables are seen on the path, but no reroute occurs until holddown expires.
Conditions: This symptom is seen under the following conditions:
- MC reroutes traffic-class out a particular path (BR/external interface) due to an OOP condition on the primary path.
- Shortly after enforcement occurs, an impairment on the new primary path occurs, causing blackhole.
- PfR MC does not declare OOP on the new primary path and attempts to find a new path until the holddown timer expires, which causes traffic loss.
Workaround: Reduce the holddown timer to 90 seconds (minimum value) to minimize impact.

• CSCtx49073
Symptoms: Free space check fails and IOS core dump never completes.
Conditions: This symptom is observed when there is not enough storage media space for Cisco IOS core dump.
Workaround: Make sure there is enough storage space for Cisco IOS core dump.

• CSCtx49098
Symptoms: A crash occurs at `udb_pre_feature_unbind_cleanup`.
Conditions: This symptom is observed when a complex 3 level HQoS policy is configured on the interface and it is manipulated with changes.
Workaround: Do not manipulate the QoS policy while it is being used or avoid using the same child policy multiple times in the parent policy.
• CSCtx51420
Symptoms: After reloading the router on Cisco IOS Release 15.2(2)S (or other affected code), the router begins to crash on bootup. The following error may also be seen:
%SYS-2-NOBLOCK: printf with blocking disabled. -Process= "TPLUS", ipl= 7, pid= 459
Conditions: This symptom is observed when AAA/TACACS is configured and is operational on the device.
Workaround: Removal of AAA system accounting will prevent the crash.

• CSCtx57146
Symptoms: SIP SPAs go in the out of service state in a scaled subinterface configuration (more than 2000 subinterfaces on a single Gigabit Ethernet port).
Conditions: This symptom occurs while performing ISSU between the iso1-rp2 and iso2-rp2 Cisco IOS XE Release 3.6S throttle image. After ISSU runversion, the SIP SPAs go in the out of service state. This issue is seen in a heavily scaled configuration. This issue is observed when there are 2000 to 3000 subinterfaces on a single SPA and the following limits are exceeded:
Overall Dual stack VRFs per box : 2800
Dual stack limit on interface : 1000
Workaround: This issue is not seen in the following scenario:
1. Before doing a load version from RP0 (initial active), issue the following command:
   asr1000# show ipv6 route table | inc IPv6
2. Note down the number of IPv6 route tables in the system.
3. Do a load version.
4. Wait for standby to come up to Standby hot.
5. Enable the standby console from RP0 (active).
   asr1000#configure terminal
   Enter configuration commands, one per line.
   End with CNTL/Z.
   asr1000(config)#
asr1000(config)#redundancy
   asr1000(config-red)#main-cpu
   asr1000(config-r-mc)#standby console enable
6. Log in to the standby console and issue the following command:
   asr1000-stby# show ipv6 route table | inc IPv6
Then, note down the number of IPv6 route tables in standby. If the number is less than the number noted at step 2, wait for some time and reverify till it reaches the number noted in step 2.
7. Issue ISSU runversion from RP0 (active).

• CSCtx57784
Symptoms: Device crashes while configuring “logging persistent url”.
Conditions: This symptom occurs when the destination file system has zero free bytes left.
Workaround: There is no workaround.
- **CSCtx62138**
  Symptoms: Standby resets continuously due to Notification timer that Expired for RF Client: Cat6k QoS Manager.
  Conditions: This symptom is observed on a Cisco 7600 HA loaded with scale QoS and GRE + IPsec configurations.
  Workaround: There is no workaround.

- **CSCtx67474**
  Symptoms: An update message is sent with an empty NLRI when the message consists of a 2-byte aspath in ASPATH attribute and a 4-byte value aggregate attribute.
  Conditions: This symptom can occur when there is a mix of 2-byte and 4-byte attributes in the update message and the message is sent from a 2-byte peer and there is a 4-byte aggregator attribute.
  Workaround: Move all the 2-byte AS peers to a separate update-group using a nonimpacting outbound policy like “advertisement-interval”.

- **CSCtx73691**
  Symptoms: The Cisco ASR 903 router forwards packets while in HSRP standby mode.
  Conditions: This symptom occurs when the Cisco ASR 903 is running HSRP and the HSRP session flaps.
  Workaround: There is no workaround.

- **CSCtx74051**
  Symptoms: When doing an ISSU downgrade, IPv6 flexible netflow monitors may be displayed and the running configuration is shown with incorrect sub-traffic types.
  Conditions: This symptom occurs upon a downgrade to Cisco IOS Release 15.2(1)S (Cisco IOS XE Release 3.5S). The monitors affected are those applied to IPv6. For example, CLI such as:

    ```
    interface fa0/0/0
    ipv6 flow monitor monitor-name input
    ```

  Workaround: Netflow code should still capture packets as expected on Cisco IOS Release 15.2(1)S. However, a reboot of the device should be done before saving the running configuration as the affected configuration saved will be incorrect and so will then fail to work on startup.

- **CSCtx74342**
  Symptoms: After an interface goes down or is OIRed in a routing table, you can temporarily see IPv6 prefixes associated with the down interface itself (connected routes) as OSPFv3 with the next-hop interface set to the interface that is down.
  Conditions: This symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 seconds default).
  Workaround: Configuring the SPF throttle timer can change the interval.
  Further Problem Description: Here is an example of output after Ethernet0/0 goes down:

    ```
    Router show ipv6 route
    IPv6 Routing Table - default - 2 entries
    Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
           B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
           IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
           ND - ND Default, NdP - ND Prefix, DCE - Destination, NDr - Redirect
           1 - LISP
           O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
    ```
CSCtx80078
Symptoms: Packets are getting punted to the CPU or being forwarded with EVC MAC security.
Conditions: This symptom is seen with implicit deny of packets with routable IPv4 header.
Workaround: There is no workaround.

CSCtx82775
Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.
Conditions: This symptom is observed when MTP is invoked for calls.
Workaround: Reload the router or perform a no sccp/sccp.

CSCtx85247
Symptoms: An ES20 line card is reset on doing redundancy switchover of RSPs.
Conditions: This symptom is seen with redundancy switchover of RSPs.
Workaround: There is no workaround.

CSCtx85489
Symptoms: A memory leak is followed by a router crash.
Conditions: This symptom is observed with a Cisco 7600 router that is running Cisco IOS Release 15.2(2)S. Configuring and unconfiguring PBR “N” number of times from an interface triggers the crash. The root cause for this issue is that each time when PBR is configured and unconfigured, memory is leaked.
Workaround: There is no workaround.

CSCtx90705
Symptoms: Several MPLS features fail for ping.
Conditions: This symptom is observed during ISSU downgrade.
Workaround: There is no workaround.

CSCtx91831
Symptoms: IP address of the SVI interface is not installed in the routing table.
Conditions: When we have an IP address configured for the BD, the following sequence of configurations puts the box in a state where the corresponding IP address is not installed in the routing table.

```
no vlan <vlan-id>     --- same as the BD
Int vlan <vlan-id>
    shutdown         --- At this point the Int vlan goes down
    no shutdown
vlan <vlan-id>
```

This issue seen only when we have SVI and BD EFP and will not be seen for SVI and trunk ports.
Workaround: A shut/no shut of the interface VLAN after adding the `vlan vlan-id` command fixes the problem.
• CSCtx94279
Symptoms: A line card crashes.
Conditions: This symptom is observed in switch traffic and flood traffic (line rate and less than 128-byte packet size) with more than one port in the egress path flood.
Workaround: There is no workaround.

• CSCtx94772
Symptoms: xconnect cannot be configured on an SVI when an RFP having the same BD is configured with pop 2 symmetric.
Conditions: This symptom is observed only when EFP is configured first and then the xconnect over SVI.
Workaround: Configure the xconnect over SVI before configuring the RFP with the same pop 2 and same BD.

• CSCty05150
Symptoms: After SSO, an ABR fails to generate summary LSAs (including a default route) into a stub area.
Conditions: This symptom occurs when the stub ABR is configured in a VRF without “capability vrf-lite” configured, generating either a summary or default route into the stub area. The issue will only be seen after a supervisor SSO.
Workaround: Remove and reconfigure “area X stub”.

• CSCty06191
Symptoms: When an IPHC configuration is applied on a multilink bundle interface and the interface is flapped, the IPHC configuration does not apply successfully on a linecard.
Conditions: This symptom is observed with a multilink interface flap.
Workaround: Unconfigure and then reconfigure the IPHC configuration on the multilink interface.

• CSCty08070
Symptoms: The router may print an error message and traceback similar to the following example:
%SCHED-STBY-3-THRASHING: Process thrashing on watched boolean 'OSPFv3 Router boolean'. -Process= "OSPFv3R-10/4/2", ipl= 5, pid= 830router ospf -Traceback= 7235C3Cz 7235F1Cz 6A5F7A8z 6A6168Cz 50DA290z 50D3B44zv
Conditions: This symptom is observed when the affected OSPFv3 router is configured, but the process does not run because it has no router-id configured. Further, an area command is configured, for example, “area X stub”.
Workaround: Configure “router-id” so that the process can run.

• CSCty14596
Symptoms:
1. PIM neighbor is not established over routed pseudowire.
2. PW cannot pass PIM traffic when destination LTL in DBUS header is 0x7ff8.
Conditions: These symptoms are seen under the following conditions:
   - Configure PIM over a routed pseudowire.
   - The core facing card is ES+.
   - The outgoing interface of the PW is a TE tunnel over the physical interface.
- Cisco IOS 15.0(1)S and later releases.

Workaround: Make the outgoing interface of PW:
1. Over a physical interface only (that is, without a tunnel).
2. TEFRR over the port-channel interface.
3. This issue will not be observed on ES20.
4. This issue will not be observed in Cisco IOS Release 15.0(1)S and later releases.

- CSCty16620
  Symptoms: The backup pseudowire in SVIEoMPLS does not come up after reloading the router.
  Conditions: This symptom is seen under the following conditions:
  1. Remote PE on the backup PW does not support pseudowire status TLV.
  2. The "no status TLV" is not configured in pw-class used in the PW, which does not support pseudowire status TLV.

Workaround:
  Proactive workaround: Configure "no status TLV" into the pw-class used if the remote side does not support status TLV.
  Reactive workaround: Reprovision the backup pseudowire after reload.

- CSCty17538
  Symptoms: IP and IPv6 traffic may be dropped when “cts role-based sgt-map” is configured.
  Conditions: This symptom is observed with nonhardware and non-CEF-switched traffic egressing an interface when an sgt-map is configured with a more specific prefix than the interface’s prefix.

Workaround: Configure the mask of the sgt-map to match that of the interface’s address.

- CSCty23747
  Symptoms: MAC address withdrawal messages are not being sent.
  Conditions: This symptom is seen with flapping REP ports on UPE.
  Workaround: There is no workaround.

- CSCty24606
  Symptoms: Under certain circumstances, the Cisco ASR 1000 series router’s ASR CUBE can exhibit stale call legs on the new active after switchover even though media inactivity is configured properly.
  Conditions: This symptom is observed during High Availability and box to box redundancy, and after a failover condition. Some call legs stay in an active state even though no media is flowing on the new active. The call legs can not be removed manually unless by a manual software restart of the whole chassis. The call legs do not impact normal call processing.
  Workaround: There is no workaround.

- CSCty28384
  Symptoms: The police actions are not accepted if given in different commands.
  Conditions: This symptom occurs if police actions are given in different commands, and they are not accepted.
  Workaround: Configure the police actions in a single command.
• CSCty28796
Symptoms: The `show snmp mib | in flash` command on the router does not show any flash entries. Also, `snmpwalk` for flash objects shows the following error:

"No Such Object available on this agent"

Conditions: This symptom is observed on Cisco ME3600X and ME3800X.
Workaround: There is no workaround.

• CSCty30886
Symptoms: A standby RP reloads.

Conditions: This symptom is observed when bringing up PPPoE sessions with a configured invalid local IP address pool under a virtual-template profile and “aa authorization network default group radius” on the box with no radius present. No IP address is assigned to the PPPoE Client.

Workaround: There is no workaround.

• CSCty32728
Symptoms: CPU hog is seen when an MVPN configuration is replaced with another using the `configure replace` command.

Conditions: This symptom is observed on a stable MVPN network when replacing the configuration with dual-home receiver/source configuration once the router comes up with the tunnel.

Workaround: There is no workaround.

• CSCty34200
Symptoms: In an MVPN scale environment, a crash is observed after “no ip multicast-routing”. A memory leak is observed after changing the data MDT address.

Conditions: This symptom is seen in an MVPN scale scenario.

Workaround: There is no workaround.

• CSCty37445
Symptoms: A DMVPN hub router with a spoke which is an EIGRP neighbor. The spoke receives a subnet from the hub and then advertises it back to the hub, bypassing split horizon.

Conditions: This symptom is observed when on the spoke you have a `distribute list route-map` command setting tags.

Workaround: Once you remove that command, EIGRP works normally.

• CSCty42626
Symptoms: Certificate enrollment fails for some of the Cisco routers due to digital signature failure.

Conditions: This symptom was initially observed when the Cisco 3945 router or the Cisco 3945E router enrolls and requests certificates from a CA server.

This issue potentially impacts those platforms with HW crypto engine. Affected platforms include (this is not a complete/exhaustive list) the Cisco c3925E, c3945E, c2951, c3925, c3945, c7200/VAM2+/VSA, possibly VPNSPA on c7600/Catalyst 6000, 819H, and ISR G2 routers with ISM IPSec VPN accelerator.

Workaround: There is no workaround.

• CSCty45999
Symptoms: The “aps group acr 1” line disappears after power off on a Cisco 7600 router in working and protection groups.
Conditions: This symptom occurs when the Cisco 7600 router suddenly loses power, and the “aps group acr 1” line does not appear again. If you run the `show controller SONET 1/1/0` command, you will see every E1 on “unconfigured” status.

Workaround: Delete the “aps protect 1 X.X.X.X” and “aps working 1” lines. The “framing” must be changed in order to delete every E1 channel configuration, then “framing” should be configured as it was in the beginning. Then, “aps group acr 1” line is configured and “aps protect 1 X.X.X.X” and “aps working 1” lines. Finally, every E1 must be configured as it was before this issue occurs. You can copy the E1 configuration before to delete anything and then paste it at the end.

- **CSCty46273**
  Symptoms: A router configured with the Locator ID Separation Protocol (LISP) may crash when the connected routes in the RIB flap.
  Conditions: This symptom is observed when LISP tracks the reachability of routing locators (RLOCs) in the RIB. For the crash to occur, a locator being watched by LISP must be covered by a route that is itself covered by a connected route. If both these routes are removed from the RIB in close succession, there is a small possibility that the race-condition resulting in this crash may be hit.
  Workaround: There is no workaround.

- **CSCty49656**
  Symptoms: A crash is observed when executing the `no ip routing` command.
  Conditions: This symptom is observed under the following conditions:
  1. Configure OSPF.
  2. Enable multicast.
  3. Create several (>6000) routes in the network to be learned by OSPF.
  4. Wait for OSPF to learn all the (>6000) routes from the network.
  Finally, executing the `no ip routing` command may crash the box.
  Workaround: There is no workaround.

- **CSCty51088**
  Symptoms: On a Cisco ME 3600X or Cisco ME 3800X, when traffic for a group (S2,G) is sent to an interface that is already acting as the source for another group (S1,G), it does not receive any traffic since no (S2,G) entry is formed.
  Conditions: This symptom is observed when the receiver interface is already a source interface for another multicast stream.
  Workaround: There is no workaround.

- **CSCty52047**
  Symptoms: IKE SAs are not getting deleted by DPD (crypto isakmp keepalive).
  Conditions: This symptom is observed on a Cisco ASR 1000 router with DPD enabled.
  Workaround: Manually delete the stuck isakmp session:
  ```
  clear crypto isakmp conn-id
  ```
  You can get the conn-id from the output of the `show crypto isakmp sa` command.

- **CSCty53654**
  Symptoms: Traffic through 6RD tunnel is getting dropped. In the `show mls cef ipv6 prefix detail` command, the `vlan vlanid` field will be present. On the ES+ line card, the `show platform npc 6rd egress-table vlan vlanid` command does not produce any output.
Conditions: This symptom occurs when using the `clear ipv6 neighbors` command.
Workaround: There is no workaround.

- CSCty54319
  Symptoms: OSPF and protocols using 224.0.0.x will not work btw CE-CE over a VLAN.
  Conditions: This symptom occurs when IGMP snooping is disabled.
  Workaround: Toggle IGMP snooping two times.

- CSCty54885
  Symptoms: The Standby RP crashes when the Active RP is removed to do a failover.
  Conditions: This symptom is observed when the last switchover happens with redundancy forced-switchover.
  Workaround: Do a switchover only with redundancy forced-switchover instead of removing the RP physically.

- CSCty58656
  Symptoms: A Cisco 7600 series router with ES+ module may crash.
  Conditions: This symptom is observed with the QoS policy map that has a name hash that is the same as an existing policy used by the ES+ module and configuring a child policy or adding a child policy that is already in use.
  Workaround: Do not call a child policy map.

- CSCty60467
  Symptoms: SSM ID leak issues or SSM stats show unprovisioned segment counters. The leak can be observed with the command `show ssm stats`. Look for the following in the output:

  Segment States Counters
  Type Class State Count
  IP-SIP SSS Unprov 1050  <<< the count indicates the IDs are getting leaked.

  Alarm: Counter reaches 1 Million: indicates you may be nearing ID exhaust state.

  Conditions: This symptom is observed with the following steps:
  1. Configure “ip dhcp ping packets 10” on an ISG.
  2. Initiate an L2-connected ISG DHCP session by triggering DHCP discover from the client.
  3. Start TCP traffic from the client immediately.
  4. The issue can be observed commonly on high CPS (greater than best practice).
  5. This issue is observed in Cisco IOS XE Release 3.2S and Cisco IOS XE Release 3.5S.
  Workaround: Configuring “ip dhcp ping packets 0” will bring down the rate of SSM ID leak.

- CSCty61212
  Symptoms: The removal of crypto map hangs the router.
  Conditions: This symptom is observed with the removal of GDOI crypto map from the interface.
  Workaround: There is no workaround.

- CSCty67401
  Symptoms: When traffic arriving on the ingress EVC BD interface is priority-tagged, the cos value of traffic egressing out of EVC with single-encap configuration is incorrectly set to 0.
Conditions: This symptom is observed on the Cisco ME3600 2RU, running Cisco IOS Release 15.2(2)S, when the cos value of a packet going out of the EVC BD port with single-encap is incorrectly set to 0.

Workaround: There is no workaround at present.

- **CSCty68348**

Symptoms: If the OSPF v2 process is configured with the `nsr` command for OSPF nonstop routing, (seen after shutdown/no shutdown of the OSPF process), the neighbor is seen on standby RP as FULL/DROTHER, although the expected state is FULL/DR or FULL/BDR. As a result, after switchover, routes pointing to the FULL/DROTHER neighbor may not be installed into RIB.

Conditions: This symptom is observed under the following conditions:

- The OSPF router is configured for “nsr”.
- Shutdown/no shutdown of the OSPF process.

Workaround: Flapping of the neighbor will fix the issue.

- **CSCty68402**

Symptoms: NTT model 4 configurations are not taking effect.

Conditions: This symptom occurs under the following conditions:

```plaintext
policy-map sub-interface-account
class prec1
   police cir 4000000 conform-action transmit exceed-action drop account
class prec2
   police cir 3500000 conform-action transmit exceed-action drop account
class prec3
   account
   class class-default fragment prec4
   bandwidth remaining ratio 1
   account

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

Workaround: There is no workaround.

- **CSCty69631**

Symptoms: Multicast RPF failures are observed with GRE tunnels and MSDP in the Cisco ASR 1000 router. This issue may occur when multicast traffic flows over GRE tunnels. This issue does not occur consistently.
Conditions: This symptom occurs when multicast traffic flows through the GRE interface.
Workaround: Reload the Cisco ASR 1000 box.

- CSCty71843
  Symptoms: Tracebacks observed at lfd_sm_start and lfd_sm_handle_event_state_stopped APIs during router bootup.
  Conditions: This symptom is observed with L2VPN (Xconnect with MPLS encapsulation) functionality on a Cisco 1941 router (acting as edge) running Cisco IOS interim Release 15.2(3.3)T. This issue is observed when a router is reloaded with the L2VPN configurations.
  Workaround: There is no workaround.

- CSCty73142
  Symptom: An IPC Init failure occurs during downgrade, which makes the standby reload continuously.
  Conditions: This symptom occurs when you perform an ISSU downgrade from Cisco IOS XE Release 3.6S to Cisco IOS XE Release 3.5.1S or Cisco IOS XE Release 3.5S.
  Workaround: There is no workaround.

- CSCty73817
  Symptoms: In large-scale PPPoE sessions with QoS, the Standby RP might reboot continuously (until the workaround is applied) after switchover. This issue is seen when the QoS Policy Accounting feature is used. When the issue occurs, the Active RP remains operational and the Standby RP reboots with the following message:
  %PLATFORM-6-EVENT_LOG: 43 3145575308: *Mar 16 13:47:23.482: %QOS-6-RELOAD: Index addition failed, reloading self
  Conditions: This symptom occurs when all the following conditions are met:
  1. There is a large amount of sessions.
  2. The QoS Policy Accounting feature is used.
  3. Switchover is done.
  Workaround: Bring down sessions before switchover. For example, shut down the physical interfaces that the sessions go through, or issue the Cisco IOS command clear pppoe all.

- CSCty74129
  Symptoms: The router may cause REP to reconverge during RSP switchover.
  Conditions: This symptom occurs when REP traffic is passing between two Cisco ASR 903 routers and you perform an RSP switchover.
  Workaround: There is no workaround.

- CSCty76106
  Symptoms: A crash is seen after two days of soaking with traffic.
  Conditions: This symptom occurs with node acting as ConPE with multiple services like REP, MST, L3VPN, L2VPN, constant frequent polling of SNMP, RCMD, full scale of routes, and bidirectional traffic.
  Workaround: There is no workaround.

- CSCty79381
  Symptoms: MST fails to peer and displays Dispute State, causing traffic loss.
Conditions: This symptom is observed upon SSO.
Workaround: To enable the port, reconfigure MST or flap the ports.

- CSCty81700
Symptoms: When a remote PE reloads in an MVPN network, it causes a memory leak.
Conditions: This symptom occurs when core interface flap or remote PE node reloads, causing a small amount of memory leak. If the node stays up experiencing a lot of core interface/remote PE outages, it can run out of memory and fail to establish PIM neighborship with remote PEs.
Workaround: There is no workaround. As a proactive measure, the user can periodically (depending on n/w outages) run the `show memory debug leak chunk` command and reload the node, if there are a lot of memory leaks reported by this command.

- CSCty82888
Symptoms: Removing an ATM Permanent Virtual Path (PVP) by the `no atm pvp` command while it is configured with the `xconnect` command causes a memory leak. This can be observed using the `show circuit memory` command:

```
Router#show acircuit memory | include AC ctx chunks
AC ctx chunks             :        200/32820      (  0%) [      2] Chunk
```

Also, on a dual-RP system with stateful switchover enabled, if the PVP is immediately reconfigured and the `xconnect` command is added, the standby RP may reload.
Conditions: These symptoms have been observed on Cisco routers that are running Cisco IOS Release 15.2(2)S.
Workaround: Unconfigure the xconnect using the `no connect` command before removing the PVP.

- CSCty83357
Symptoms: ACL denied packets are getting punted to host queue, leading to flaps in routing protocols.
Conditions: This symptom occurs when ACL is configured with src IP match, and packets are being denied by the ACL. The packets are punted to the CPU.
Workaround: There is no workaround.

- CSCty85634
Symptoms: A router configured with the Locator ID Separation Protocol (LISP) without an EID-table for the default VRF fails to maintain its LISP map-cache during an RP switchover. After the switchover, the existing remote EID entries in CEF eventually expire and new data packet signals result in repopulation of the LISP map-cache, thus resuming normal operation.
Conditions: This symptom occurs in a LISP configuration that contains EID-tables for VRFs other than the default and does not contain an EID-table for the default VRF.
Workaround: Configure an EID-table for the default VRF before the switchover with some LISP configuration such as “ipv4 itr”.

- CSCty91955
Symptoms: L2-switched traffic loss within a BridgeDomain routed traffic via an SVI experiences no loss.
Conditions: This symptom occurs with BridgeDomain that has both tagged and untagged EVCs.
Issue should not happen with like-to-like scenario.
Workaround: Make sure there is like-to-like (tagged-to-tagged or untagged-to- untagged) communication.
CSCty93290
Symptoms: Momentary traffic loss of multicast traffic with QoS configuration on EFP is observed.
Conditions: This symptom is seen under the following conditions:
1. Have multiple VLANs in the OIF list.
2. Each VLAN should have only one EFP/sp.
3. Have QoS configured on EFPs.
Workaround: There is no workaround.

CSCty94289
Symptoms: The drop rate is nearly 1 Mbps with priority configuration.
Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.
Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the Flexwan line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

CSCty96049
Symptoms: The Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.
Conditions: This symptom is observed with the Cisco IOS Software that contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.
Workaround: Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp
Note: The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2012 bundled publication.
Individual publication links are in “Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication” at the following link: http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html
PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C
CVE ID CVE-2012-4621 has been assigned to document this issue.
Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
• CSCty96263
Symptoms: Under periods of transient interface congestion, an MPLS-TP network may experience
unnecessary traffic switchovers or longer than expected restoration times.
Conditions: This symptom is observed during periods of transient interface congestion. This
behavior will be caused by loss of pseudowire status packets. Lack of a classification mechanism
for these packets prevents user from protecting them with a QoS policy.
Workaround: There is no workaround.

• CSCty96579
Symptoms: Under periods of transient interface congestion, an MPLS-TP network may experience
unnecessary traffic switchovers or longer than expected restoration times.
Conditions: This symptom is observed during periods of transient interface congestion. This
behavior will be caused by loss of vital OAM packets (for example. AIS/LDI, LKR). Lack of a
classification mechanism for these packets prevents from protecting them with a QoS policy.
Workaround: There is no workaround.

• CSCty99331
Symptoms: CPU hog messages are seen on the console.
Conditions: This symptom is seen when applying huge rmap with more than 6k sequences on an
interface.
Workaround: There is no workaround.

• CSCty99711
Symptoms: SIP-400 crash may be observed due to illegal memory access.
Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SRE4 when SIP-400 has
PPPoE session scale.
Workaround: There is no workaround.

• CSCtz01361
Symptoms: Traffic gets blackholed when TE auto-backup is enabled on the midpoint router and FFR
is configured on the P2MP TE tunnel headend.
Conditions: This symptom is seen when enabling FRR on the headend with auto-backup already
configured on the box.
Workaround: Remove the auto-backup configuration from the midpoint router.

• CSCtz03779
Symptoms: The standby RSP crashes during ISSU.
Conditions: This symptom occurs when you perform an ISSU downgrade from Cisco IOS XE
Release 3.6S to Cisco IOS XE Release 3.5S.
Workaround: There is no workaround.

• CSCtz04090
Symptoms: In a VRRP/HSRP setup, traffic from particular hosts is getting dropped. Ping from the
host to any device through the VRRP routers fails.
Conditions: This symptom is usually seen after a VRRP/HSRP switchover. The packet drops
because of some packet loop that is created between the routers running VRRP/HSRP.
Workaround: A clear of the MAC table on the new VRRP master usually restores the setup to
working conditions.
• CSCtz13451
Symptoms: A Cisco ME 3800X and Cisco ME 3600X switch may experience CPU HOG errors and then a watchdog crash or memory corruption.
Conditions: This symptom is observed when running many of the `show platform mpls handle` commands. The switch may crash.

```
SW#sh platform mpls handle 262836664 ?
BD_HANDLE              bd/el3idc_vlan handle
L2VPN_L2_HANDLE        l2 tunnel intf handle
L2VPN_FW_BIND_DATA    pw bind data
LFIB_TABLE             LFIB TABLE handle
PORT_HANDLE            port/met handle
RW_HANDLE              Rewrite handle
SW_OBJ_ADJACENCY       oce type SW_OBJ_ADJACENCY
SW_OBJ_ATOM_DISP       oce type SW_OBJ_ATOM_DISP
SW_OBJ_ATOM_IMP        oce type SW_OBJ_ATOM_IMP
SW_OBJ_DEAGGREGATE    oce type SW_OBJ_DEAGGREGATE
SW_OBJ_EGRESS_LABEL    oce type SW_OBJ_EGRESS_LABEL
SW_OBJ_EOS_CHOICE     oce type SW_OBJ_EOS_CHOICE
SW_OBJ_FIB_ENTRY       oce type SW_OBJ_FIB_ENTRY
SW_OBJ_FRR             oce type SW_OBJ_FRR
SW_OBJ_GLOBAL_INFO     oce type SW_OBJ_GLOBAL_INFO
SW_OBJ_ILLEGAL         oce type SW_OBJ_ILLEGAL
SW_OBJ_IPV4_FIB_TABLE  oce type SW_OBJ_IPV4_FIB_TABLE
SW_OBJ_IPV6_FIB_TABLE  oce type SW_OBJ_IPV6_FIB_TABLE
SW_OBJ_LABEL_ENTRY     oce type SW_OBJ_LABEL_ENTRY
SW_OBJ_LABEL_TABLE     oce type SW_OBJ_LABEL_TABLE
SW_OBJ_LABEL_ENTRY     oce type SW_OBJ_LOADBALANCE
SW_OBJ_RECEIVE         oce type SW_OBJ_RECEIVE
```

Workaround: Do not run the commands as they are for development use.

• CSCtz14980
Symptoms: When you perform the RP switch, the standby RP (original active one) will keep rebooting.
Conditions: This symptom is observed when you have “crypto map GETVPN_MAP gdoi fail-close” configured and image is Cisco IOS XE Release 3.6S or Cisco IOS XE Release 3.7S.
Workaround: There is no workaround.

• CSCtz16622
Symptoms: A Cisco ME 3600X acts as a label disposition Edge-LSR when receiving MPLS packets with Checksum 0xFFFF that will continue to drop with Ipv4HeaderErr and Ipv4ChecksumError at nile.
Conditions: This symptom is seen with label pop action at the Edge-LSR.
Workaround: There is no workaround.

• CSCtz23638
Symptoms: The following error message is seen on the console:

```
PLIM driver informational error txnpTooLittleData
```
Conditions: This symptom is observed when the SIP40 carrier card is present in the router, along with any of the below SPAs:
- SPA-1CHOC3-CE-ATM
- SPA-1XCHOC12/DS0
SPA-1XCHSTM1/OC3
SPA-1XCHSTM1/OC3W (Same SPA as SPA-1XCHSTM1/OC3. Included in “SB” bundles)
special pricing)
SPA-24CHT1-CE-ATM *
SPA-2CHT3-CE-ATM
SPA-2X1GE-SYNCE
SPA-2XCT3/DS0
SPA-2XT3/E3
SPA-4XCT3/DS0
SPA-4XCT3/DS0-WE (Same SPA as SPA-4XCT3/DS0. Included in “SB” bundles - special pricing)
SPA-4XT3/E3
SPA-8XCHT1/E1
SPA-DSP
SPA-WMA-K9
Workaround: There is no workaround.

- CSCtz27782
  Symptoms: A crash is observed on defaulting service instance with OFM on EVC BD configured.
  Conditions: This symptom occurs when interface is in OAM RLB slave mode.
  Workaround: There is no workaround.

- CSCtz31888
  Symptoms: After state change of one of the L3 uplink interfaces, the STP cost of BPDU PW increases from 200 to 2M, which can lead to blocking state in STP for this PW.
  Conditions: This symptom occurs with state change of one of the uplink L3 interfaces.
  Workaround: Increase the cost of the access ring to more then 2M to avoid blocking of the BPDU PW.

- CSCtz32521
  Symptoms: In interop scenarios between the Cisco CPT and Cisco ASR 9000 platforms, in order to support the transport switchover requirement for 50 msec, it would require Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.
  Conditions: This symptom occurs in interop scenarios between Cisco CPT and the Cisco ASR 9000 platform. In order to support transport switchover requirement for 50 msec, it would require the Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.
  Workaround: There is no workaround.

- CSCtz35467
  Symptoms: The QoS policy-map gets detached from the interface on line protocol down-->up transition on reload, admin shut/no shut, and interface flap as well.
  Conditions: This symptom is observed when the QoS policy-map is applied at the interface and more than one child has “priority + police cir percent x” configured.
  Workaround: To be preventive, use “police cir <absolute>” instead of “police cir percent x”. To be reactive, use EEM applet/script.
Further Problem Description: There is no error message in the syslog, but only on the console. It seems that line protocol UP can be used as the trigger action for EEM.

- **CSCtz38119**
  Symptom: The router does not complete a MAC address flush on the receiving side of a VPLS pseudowire.
  Conditions: This symptom occurs when the router receives a Layer 2 MAC withdrawal over a VPLS pseudowire.
  Workaroud: There is no workaround.

- **CSCtz40435**
  Symptoms: The L4 port-range security ACL does not work on EVC.
  Conditions: This symptom is observed when security the ACL containing L4 port range operation that is applied on EVC. The behavior is not as expected. The same works on the physical interface.
  Workaround: Add support for the L4 port range operation similar to the case of applying it on the physical interface.
  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.
  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.
  Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- **CSCtz44963**
  Symptoms: CCDB is not populated after removing/readding EFP.
  Conditions: This symptom occurs when CCDB is not populated after removing/readding EFP.
  Workaround: Reload the router.

- **CSCtz45057**
  Symptoms: High CPU is seen on a Cisco ME 3800X switch.
  Conditions: This symptom occurs when loop of OTNIFMIB causes CPU Hog/Crash on a Cisco ME 3800X switch during pulling from PPM.
  Workaround: Disable OTNIFMIB while pulling from PPM, which is not supported or required on the Cisco ME 3800X and ME 3600X switches.

- **CSCtz46300**
  Symptoms: Traffic is not classified under the QoS ACLs having port matching using the range (inclusive range), lt (less than), and gt (greater than) operators.
  Conditions: This symptom is observed with IPv4 and IPv6 with L4 port range operations using range, lt, and gt, which do not work with QoS ACLs on Cisco ME 3600 and Cisco ME3800 switches.
  Workaround: There is no workaround.

- **CSCtz54823**
  Symptoms: The configuration is getting locked on the chopper SPA.
  Conditions: This symptom occurs as follows:
  1. Shut down the controller of the SPA.
  2. Reload will bring the SPA in the locked state.
Caveats in Cisco IOS XE 3.4S Releases

Workaround: There is no workaround. Erase startup and reload the system to get back to configuration mode.

- **CSCtz74189**
  Symptoms: Occasionally, the system hangs at bootup with the following signature in the bootlogs. The system will not respond to break character keys.

```
Configuring Freq Synthesizer 2
Synthesizer PLL 2 locked successfully
Configuring Freq Synthesizer 3
Synthesizer PLL 3 locked successfully
Configuring Freq Synthesizer 4
Synthesizer PLL 4 locked successfully
TDM Processor has been configured in iter(1) <<<<<<<<<<<<<< HANG
```

Conditions: This symptom occurs in normal reload conditions, or on a next reload of the software after a system power cycle.

Workaround: Requires a system power cycle.

- **CSCtz75228**
  Symptoms: On a power cycle or a reload condition, the system may stall occasionally after the following console logs are printed.

```
<snip
Finished memctrl.h, apply WinHMS Errata...
Initialize Winpath
Initializing interrupt controller
Initialization of Winpath Complete
loading program at addr: 0xE2C00000, size: 0x0007A648
Enable the MIPS Core0
Before minimon_init() call... <<<<<<<<<<<<HANG
-----  minimon 1st 64 bytes -----
C00BD108:
```

Conditions: This symptom may occur during a system reload.

Workaround: A power cycle is required, and the subsequent reload may not be impacted.

- **CSCtz75380**
  Symptoms: A Cisco ASR 1000 series router sends malformed radius packets during retransmission or failover to a secondary radius server, for example, Cisco CAR.

ISG log if secondary radius server is installed in the network:

```
%RADIUS-4-RADIUS_DEAD: RADIUS server <ip-secondary-Radius-Server>:1645,1646 is not responding.
%RADIUS-4-RADIUS_ALIVE: RADIUS server <ip-secondary-Radius-Server>:1645,1646 is being marked alive.
```

Radius-Server Log:
13:23:01.011: P78: Packet received from 10.0.0.1
13:23:01.011: P78: Packet successfully added
13:23:01.011: P78: Parse Failed: Invalid length field - 63739 is greater than 288
13:23:01.011: Log: Packet from 10.0.0.1: parse failed <unknown user>
13:23:01.011: P78: Rejecting Request: packet failed to parse
13:23:01.011: P78: identifier = 40
13:23:01.011: P78: length = 21
13:23:01.011: P78: Sending response to 10.0.0.1
Conditions: The issue can occur during retransmission of radius access requests or if radius packets are sent to a secondary radius server.
Workaround: There is no workaround.

- CSCtz80571
  Symptoms: Rewriting the ingress tag configuration is not accepted.
  Conditions: This symptom occurs when you create a port-channel1 interface and then create a port-channel2 interface.
  Workaround: There is no workaround.

- CSCtz83311
  Symptoms: In the bootlog, the following strings may be observed:
  "MCB timeout"
  Occasionally, these messages also are followed by a Gigabit Ethernet port link down for any of the ports Gig 0/1-Gig 0/8. A shut/no shut may not recover the link down condition.
  Conditions: This symptom occurs during a system reload. It may also occur if a media-type command is issued to the first eight Gigabit Ethernet ports.
  Workaround: Do not configure “media-type rj45” for the first eight ports either at bootup time or configurations if you are using an image that does not have this fix.

- CSCtz85225
  Symptoms: The RF functionality does not work on 10GE interfaces.
  Conditions: This symptom is observed on the Cisco ASR 903 router.
  Workaround: There is no workaround.

- CSCtz88289
  Symptoms: It is observed that in a Cisco ME 3600-24CX unit, which is subjected to 100 consecutive image reloads, there is a system bootup hang in this area. The system stalls indefinitely and does not respond to console keystrokes like break keys.
  Conditions: This symptom may occur during a system bootup.
  Workaround: A powercycle is required, and the next reload may not hit the above condition.

- CSCtz94188
  Symptoms: With AdvancedMetroIPAccess evaluation license and with TDM permanent license xconnect under CEM, cktts are not shown and are not configurable.
  Conditions: This symptom occurs under regular configuration steps.
  Workaround: There is no workaround.
• CSCtz96342

Symptoms: Inconsistency in a scaled feature license name between Cisco IOS Releases 12.2(52)EY*/15.1(2)EY* and Cisco IOS Release 15.2(2)S:

Cisco IOS Releases 12.2(52)EY*/15.1(2)EY* - ScaledServices
Cisco IOS Release 15.2(2)S - ScaledMetroAggrServices

Conditions: This symptom occurs with an upgrade from Cisco IOS Releases 12.2(52)EY*/15.1(2)EY* to Cisco IOS Release 15.2(2)S, which could impact the scalability feature in below ways:

- If user already had permanent license before upgrade, it will now downgrade to Eval license.
- New license for installing ScaledMetroAggrServices cannot be generated as the license tool does not support this feature name.

Workaround: Upgrade to Cisco IOS Release 15.2(2)S1.

Resolved Caveats—Cisco IOS XE Release 3.4.4S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.4S.

• CSCto02712

Symptoms: A router that is running Cisco IOS Release 15.1(4)M1 with “proxy-arp” enabled will incorrectly reply to duplicate address detection ARP requests sourced from end devices.

Some end devices will send an ARP request for their assigned IP to check for duplicate address detection per RFC5227. When this occurs, the router should ignore this ARP request. With this issue, the router will respond to the request, which triggers the duplicate address detection on the end device and breaks connectivity between the router and end device.

Conditions: This symptom is observed with the following conditions:

- “proxy-arp” is enabled on the client-facing Layer 3 interface.
- The end device sends a “duplicate address detection” ARP request on its local subnet.

Workaround 1: Configure `no ip proxy arp` on the client-facing interface.
Workaround 2: Disable “duplicate address detection” on the end device.

• CSCto16377

Symptoms: DPD deletes only IPsec SA and not IKE SA.

Conditions: This symptom is observed when DPD is enabled and peer is down.

Workaround: Manually delete the stuck ISAKMP session by using the `clear crypto isakmp conn-id` command. You can get the conn-id from the `show crypto isakmp sa` command output.

• CSCto85731

Symptoms: A crash is seen at the nhrp_cache_info_disseminate_internal function while verifying the traffic through FlexVPN spoke-to-spoke channel.

Conditions: This symptom is observed under the following conditions:

1. Configure hub and spokes (flexvpn-nhrp-auto connect), as given in the enclosure.
2. Initiate the ICMP traffic through spoke-to-spoke channel between spoke devices.
3. Do a `clear crypto session` at Spoke1.
4. Repeat steps 2 and 3 a couple of times.
Workaround: There is no workaround.

Further Problem Description: In the given conditions, one of the spoke device crashed while sending ICMP traffic (10 packets) through FlexVPN spoke-to-spoke channel. The crash decode points to the “nhrp_cache_info_disseminate_internal” function.

- CSCtq99664
  Symptoms: Traffic does not egress from the interface.
  Conditions: This symptom is observed when the VRF set on the interface is originally configured for the IPv4 and IPv6 address family. If the VRF is reconfigured to remove the IPv4 address family, then all interfaces in that VRF stop sending traffic.
  Workaround: Shut down and re-enable the interface in question.

- CSCts16569
  Symptoms: The router might reload unexpectedly with scaled serial interfaces configuration.
  Conditions: This symptom occurs during scaling to 4000 NSR peers with 1.5M routes.
  Workaround: There is no workaround.

- CSCts27674
  Symptoms: The static route is not injected to the routing table after enabling the crypto map on the interface.
  Conditions: This symptom occurs when you configure “reverse-route static” in the crypto map.
  Workaround: Reconfigure “reverse-route static”.

- CSCts56044
  Symptoms: A Cisco router crashes while executing a complex command. For example:
  ```
  show flow monitor access_v4_in cache aggregate ipv4 precedence sort highest ipv4 precedence top 1000
  ```
  Conditions: This symptom is observed while executing the `show flow monitor top` top-talkers command.
  Workaround: Do not execute complex flow monitor top-talkers commands.

- CSCts72911
  Symptoms: In case of a GR/NSF peering, after an SSO, the restarting router (PE, in this case) does not advertise RT constrain filters to the nonrestarting peer (RR, in this case).
  Conditions: This symptom is observed after an SSO in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the nonrestarting router does not send back the corresponding VPN prefixes towards the restarted router.
  Workaround: There is no workaround.

- CSCts83046
  Symptoms: Back-to-back ping fails for P2P GRE tunnel address.
  Conditions: This symptom is observed when HWIDB is removed from the list (through `list remove`) before it gets dequeued.
  Workaround: There is no workaround.

- CSCts84132
  Symptoms: Kingpin crashes.
  Conditions: This symptom occurs during reload with a 4096 subinterface.
- **CSCtt17762**
  Symptoms: Mtrace does not show the IP address of RPF interface of a multicast hop.
  Conditions: This symptom is observed on an IP PIM multicast network.
  Workaround: There is no workaround.

- **CSCtt99627**
  Symptoms: The **lacp rate** and **lacp port priority** commands may disappear following a switchover from active to standby RP.
  Conditions: This symptom is observed with the Cisco 7600 platform.
  Before performing a switchover, one may check the configuration on the standby RP to see if the commands are present or not. If the commands are not present on the standby RP, then they will disappear if a switchover occurs.
  Workaround: Prior to switchover, if the commands do not show up on the standby RP, as described above, then unconfiguring and reconfiguring the command on the active RP will fix the issue.
  Otherwise, if the commands disappear after a switchover, then the commands must be reconfigured on the newly active RP.

- **CSCtu01601**
  Symptoms: A Cisco ASR1000 series router may crash while executing the **write memory** command.
  Conditions: This symptom may be triggered when the memory in the router is low.
  Workaround: There is no workaround.

- **CSCtu23195**
  Symptoms: SNMP ifIndex for serial interfaces (PA-4T/8T) becomes inactive after PA OIR.
  Conditions: This symptom is observed with a PA OIR.
  Workaround: Unconfigure and reconfigure the channel-groups of the controller and reload the router.

- **CSCtv36812**
  Symptoms: Incorrect crashInfo file name is displayed during a crash.
  Conditions: This symptom is observed whenever a crash occurs.
  Workaround: There is no workaround.

- **CSCtw46229**
  Symptoms: A small buffer leak is seen. The PPP LCP configuration requests are not freed.
  Conditions: This symptom is observed with PPP negotiations and the session involving PPPoA.
  Workaround: Ensure that all your PPP connections stay stable.

- **CSCtw61872**
  Symptoms: The router will crash when executing a complex sort on the flexible netflow cache from multiple CLI sessions.
  Conditions: This symptom is observed when executing a complex sort with top-talkers on a **show** command from multiple CLI sessions (note that normal **show** commands without top-talkers are fine):

  ```
  sh flow monitor QoS_Monitor cache sort highest counter packets top 1000
  ```
sh flow monitor QoS_Monitor cache sort highest counter packets top 10000

Workaround: Do not execute complex sorts with top-talkers on the `show` output from multiple CLI sessions.

- **CSCtw64073**
  Symptoms: Traceback is seen with the “%CPPOSLIB-3-ERROR_NOTIFY” error message.
  Conditions: This symptom is observed when the Cisco ASR router is processing ACL merge for a given feature set.
  Workaround: FP will crash and restart in most cases; however, in some cases a reboot may be needed.

- **CSCtw80678**
  Symptoms: Multilink PPP ping fails when the serial interfaces experience the QMOVESTUCK error.
  Conditions: This symptom may be observed if multilink PPP member links and serial interfaces on which the QMOVESTUCK error is reported are on the same SPA.
  Workaround: No shut the interface in the QMOVESTUCK error message, remove QoS policies on interface and subinterfaces, remove the interface from T1/T3 controller, and then rebuild the configuration.

- **CSCtw98200**
  Symptoms: Sessions do not come up while configuring RIP commands that affect the virtual-template interface.
  Conditions: This symptom is observed if a Cisco ASR1000 series router is configured as LNS.
  RIP is configured with the `timers basic 5 20 20 25` command. Also, every interface matching the network statements is automatically configured using the `ip rip advertise 5` command. These interfaces include the loopback and virtual-template interfaces too.
  On a Cisco ASR1000 series router, this configuration causes the creation of full VAIIs which are not supported. Hence, the sessions do not come up. On Cisco ISR 7200 routers, VA subinterfaces can be created.
  Workaround: Unconfigure the `timers rip` command.

- **CSCtx04709**
  Symptoms: Some EIGRP routes may not be removed from the routing table after a route is lost. The route is seen as “active” in the EIGRP topology table, and the active timer is “never”.
  Conditions: This symptom is seen when a multiple route goes down at the same time, and query arrives from the neighbor router. Finally, the neighbor detects SIA for the affected router and the neighbor state is flap. However, active entry is remaining after that, and the route is not updated.
  Workaround: The `clear ip eigrp topology network mask` command may remove unexpected active entry.

- **CSCtx11598**
  Symptoms: A router reload causes a Cisco Shared Port Adapter (SPA) failure with the following error message:

  `% CWAN_SPA-3-FAILURE: SPA-2CNT3-CE-ATM[2/2]: SPA failure`

  This failure can cause the SPA to go to one of the following states:
  - none
- standby reset
- down

This failure leads to unexpected system reload.

Conditions: This symptom is observed during router reload for 15-20 times.

Workaround: Ensure that all of the library shared objects are loaded at the time of the SPA initialization.

- CSCtx19332

Symptoms: A Cisco router crashes when “remote mep” is unlearned while auto EOAM operations are executing.

Conditions: This symptom is observed if “remote mep” is unlearned from the auto database (shutdown on interface or remote mep reload) while the “IP SLA ethernet-monitor jitter” operation is still running. The crash occurs if the initial control message times out.

Workaround: There is no workaround.

- CSCtx32329

Symptoms: When using the `show ipv6 rpf` command, the router crashes or displays garbage for RPF idb/nbr.

Conditions: This symptom can happen when the RPF lookup terminates with a static multicast route that cannot be resolved.

Workaround: Do not use static multicast routes, or make sure that the next-hop specified can always be resolved. Do not use the `show` command.

- CSCtx32599

Symptoms: Traceback messages are printed on the console. The device does not experience adverse effects.

Conditions: This symptom occurs on the console.

Workaround: There is no workaround.

- CSCtx45373

Symptoms: Under `router eigrp virtual-name` and `address-family ipv6 autonomous-system 1`, when you enter `af-interface Ethernet0/0` to issue a command and exit, and later, under `router bgp 1` and `address-family ipv4 vrf red`, you issue the `redistribute ospf 1` command, the “VRF specified does not match this router” error message is displayed. When you issue the `redistribute eigrp 1` command, it gets NVGENd without AS number.

Conditions: This symptom occurs under `router eigrp virtual-name` and `address-family ipv6 autonomous-system 1`, when you enter `af-interface Ethernet0/0` to issue a command and exit, and later, under `router bgp 1` and `address-family ipv4 vrf red`, you issue the `redistribute ospf 1` command.

Workaround: Instead of using the `exit-af-interface` command to exit, if you give a parent mode command to exit, the issue is not seen.

- CSCtx66046

Symptoms: The Standby RP crashes with a traceback listing `db_free_check`.

Conditions: This symptom occurs when OSPF NSR is configured. A tunnel is used and is unnumbered with the address coming from a loopback interface. A network statement includes the address of the loopback interface. This issue is seen when removing the address from the loopback interface.
**Workaround:** Before removing the address, remove the network statement which covers the address of the loopback interface.

- **CSCtx66804**
  Symptoms: The configuration “ppp lcp delay 0” does not work and a router does not initiate CONFREQ.
  Conditions: The symptom is observed with the following conditions:
  - “ppp lcp delay 0” is configured.
  - The symptom can be seen on Cisco IOS Release 15.0(1)M5.
  Workaround: Set delay timer without 0.

- **CSCtx74342**
  Symptoms: After the interface goes down or is OIRed, in a routing table, you can temporarily see IPv6 prefixes associated with the down interface itself (connected routes) as OSPFv3 with the next-hop interface set to the interface that is down.
  Conditions: This symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 sec default).
  Workaround: Configuring SPF throttle timer can change the interval.

Further Problem Description: Here is an example of output after Ethernet0/0 goes down:

```
Router# show ipv6 route
IPv6 Routing Table – default – 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DC - Destination, NDr - Redirect
       1 - LISP
       0 - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O  2001::/64 [110/10] via Ethernet0/0, directly connected
```

- **CSCtx81689**
  Symptoms: In case of IPv6MVPN, PIM neighbor cannot be established.
  Conditions: This symptom is only triggered on FP40 or above systems.
  Workaround: Disable MLRE with the `platform multicast lre off` configuration command.

- **CSCtx84948**
  Symptoms: A Cisco ASR 1000 series router malfunctions after consecutive ESP crashes triggered by CSCtr56576. This symptom is observed when the interfaces are up/up but are not sending traffic. You can also identify this state using the following command:

  ```
  Router# show platform software interface fp active name GigabitEthernet5/0/0
  Name: GigabitEthernet5/0/0, ID: 23, QFP ID: 22, Schedules: 4096
  Type: PORT, State: disabled, SNMP ID: 16, MTU: 1500            
  The output of the command indicates that at the ESP level, the interface is disabled and cannot forward traffic.
  Conditions: This symptom is observed when the Cisco ASR 1000 series router has redundant ESPs and consecutive ESP crashes. This symptom has been caused only by CSCtr56576.
  Workaround: Shut/no shut the disabled interface to resume the traffic.
  ```
• CSCtx89260
  Symptoms: Adding the deleted port channel interface is not initializing the snmp-index.
  Conditions: This symptom is observed when adding the deleted port-channel interface.
  Workaround: Reloading the standby and then doing an RP switchover or doing a double RP switchover corrects the configuration.

• CSCty03745
  Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.
  Conditions: This symptom occurs when the IPv4 default route exists, that is:
  
ip route 0.0.0.0 0.0.0.0 <next-hop>

Or a certain static/IGP route exists. For example:

  
ip route 0.0.253.0 255.255.255.0 <next-hop>

  Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family.
  For example:
  
router bgp 65000
  address-family l2vpn vpls
  neighbor 10.10.10.10 next-hop-self

  Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

• CSCty05092
  Symptoms: EIGRP advertises the connected route of an interface which is shut down.
  Conditions: This symptom is observed under the following conditions:
  1. Configure EIGRP on an interface.
  2. Configure an IP address with a supernet mask on the above interface.
  3. Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.
  Workaround 1: Remove and add INTERFACE VLAN xx.
  Workaround 2: Clear ip eigrp topology x.x.x.x/y.

• CSCty05150
  Symptoms: After SSO, an ABR fails to generate summary LSAs (including a default route) into a stub area.
  Conditions: This symptom occurs when the stub ABR is configured in a VRF without “capability vrf-lite” configured, generating either a summary or default route into the stub area. The issue will only be seen after a supervisor SSO.
  Workaround: Remove and reconfigure “area x stub”.

• CSCty06191
  Symptoms: When an IPHC configuration is applied on a multilink bundle interface and the interface is flapped, the IPHC configuration does not apply successfully on a line card.
  Conditions: This symptom is observed with a multilink interface flap.
  Workaround: Unconfigure and then reconfigure the IPHC configuration on the multilink interface.
• CSCty10285
  Symptoms: WCCP redirection does not happen with a Cisco ASR 1000 router running Cisco IOS XE Release 3.5 RP1.
  Conditions: This symptom occurs when GetVPN is used.
  Workaround: There is no workaround.

• CSCty19713
  Symptoms: The ESP or CPP of a Cisco ASR 1000 series router crashes.
  Conditions: This symptom is observed in the NAT Application Layer Gateway (ALG) for DNS packets.
  Workaround: There is no workaround.

• CSCty21638
  Symptoms: The Cisco 3945 router crashes with the base configuration of SAF/EIGRP.
  Conditions: This symptom occurs when enabling the SAF Forwarder on the Cisco 3945 router box.
  Workaround: There is no workaround.

• CSCty24606
  Symptoms: Under certain circumstances, the Cisco ASR 1000 series router’s ASR CUBE can exhibit stale call legs on the new active after switchover even though media inactivity is configured properly.
  Conditions: This symptom is observed during High Availability and box to box redundancy, and after a failover condition. Some call legs stay in an active state even though no media is flowing on the new active. The call legs cannot be removed manually unless by a manual software restart of the whole chassis. The call legs do not impact normal call processing.
  Workaround: There is no workaround.

• CSCty32851
  Symptoms: A Cisco router may unexpectedly reload due to software forced crash exception when changing the encapsulation on a serial interface to “multilink ppp”.
  Conditions: This symptom is observed when the interface is configured with a VRF.
  Workaround: Shut down the interface before making the encap configuration change.

• CSCty54885
  Symptoms: The Standby RP crashes when the Active RP is removed to do a failover.
  Conditions: This symptom is observed when the last switchover happens with redundancy forced-switchover.
  Workaround: Do a switchover only with redundancy forced-switchover instead of removing the RP physically.

• CSCty63356
  Symptoms: Memory leak is seen in the cpp_sp_svr process on ESP.
  Conditions: This symptom is observed under the following conditions:
  - A topology of dVTI IPsec as below:
    
    \[
    \text{dVTI Server (ASR1k)} \quad \text{---} \quad \text{dVTI Client [CES] (7200)}
    \]
  - Scale 1000 IKE * 1 VRF * 4 IPsec, total 4K IPsec sessions.
- Multi-SA enable.
- CAC=50,DPD=60/15/periodic.
- Reload CES (7200 platform) every ~20 minutes.
- ~60M bidirectional traffic.

Workarounds:

**CSCty68348**

Symptoms: If the OSPF v2 process is configured with the `nsr` command for OSPF nonstop routing, (seen after shutdown/no shutdown of the OSPF process), the neighbor is seen on standby RP as FULL/DROTHER, although the expected state is FULL/DR or FULL/BDR. As a result, after switchover, routes pointing to the FULL/DROTHER neighbor may not be installed into RIB.

Conditions: This symptom is observed under the following conditions:
- The OSPF router is configured for “nsr”.
- Shutdown/no shutdown of the OSPF process.

Workaround: Flapping of the neighbor will fix the issue.

**CSCty78435**

Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.

Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

**CSCty94289**

Symptoms: The drop rate is nearly 1 Mbps with priority configuration.

Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.

Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the Flexwan line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

**CSCty96049**

Symptoms: Several Cisco 3750X switches in a stack crash. The crashinfo shows vector 0x200 and stack corruption:

```
C3750E Software (C3750E-UNIVERSALK9-M), Version 15.0(1)SE2, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Compiled Thu 22-Dec-11 00:05 by prod_rel_team
Signal = 10, Vector = 0x200, Uptime = E
.
.
--------- Stack Dump -----------------------
Stack Frame Pointer in Context is 0x46DCB0C, at process level
 : INVALID STACK ADDRESS
```
Conditions: The symptom is observed when the switch receives a DHCP using a TLV with a length of 256 or longer. This is not platform-specific.

Workaround: As a workaround, an administrator can disable the DHCP device classifier using the `device-sensor filter-spec dhcp exclude all` command, as shown in the following example:

```
hostname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
hostname(config)# device-sensor filter-spec dhcp exclude all
hostname(config)# end
```

- **CSCty96052**

  Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.

  Conditions: This symptom is an extreme corner case/timing issue. This issue has been observed only once on the release image.

  Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- **CSCtz13465**

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

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

  Workaround: There is no workaround.

- **CSCtz13818**

  Symptoms: In a rare situation when route-map (export-map) is updated, Cisco IOS software is not sending refreshed updates to the peer.

  Conditions: This symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then, the Cisco IOS software does not send refreshed updates with modified route-targets.

  Workaround 1: Refresh the updated route-target to use `clear ip route vrf vrf-name net mask`.

  Workaround 2: Hard clear the BGP session with the peer.

- **CSCtz25953**

  Symptoms: The “LFD CORRUPT PKT” error message is dumped and certain length packets are getting dropped.

  Conditions: This symptom is observed with a one-hop TE tunnel on a TE headend. IP packets with 256 or multiples of 512 byte length are getting dropped with the above error message.

  Workaround: There is no workaround.

- **CSCtz38558**

  Symptoms: The following traceback may be seen on a Cisco ASR 1000 router when processing some IPv6 packets.

```
Apr 18 17:20:27.554: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.0 Thread:132
TS:00000176080579214858 %INFRA-3-INVALID_GPMACCESS: Invalid GPM Load at
800268cd HAL start 3fc0 HAL end 413f INFRA start 409e INFRA 4140 NET 340d
.Traceback=18002b3a75f6cabf53c25612ed4553871e 804b0d63 804b1204 8046c212 80020708
800268cd 80026cd0 80435955 806509bb
Apr 18 17:20:27.554: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.0 Thread:132
TS:00000176080579433103 %INFRA-3-INVALID_GPMACCESS_INFO: 80026cd0 0002fdd0 0002fdd4
0002fdd0 00000002 00000001 00000001 0003413f 00000001
93b9bac0 8ba80000 fffffffd 00201000
```
Conditions: This symptom is observed when the IPv6 packet is malformed.
Workaround: There is no workaround.
Additional Information: The packet will be dropped.

- CSCtz61014
  Symptoms: The system crashes.
  Conditions: This symptom occurs when adding or deleting NTP leap second in NTP master mode.
  Workaround: Do not configure the system as NTP master.

- CSCtz67785
  Symptoms: The Cisco ASR 1000 router may experience a CPP crash.
  Conditions: This symptom occurs when the router is configured for Session Border Controller (SBC). During periods of high traffic, FP reports a lot of media up events to RP, which can crash FP.
  Workaround: If “ip nbar protocol-discovery” is enabled, it may exacerbate the crashes. Removing it may help provide some stability.

- CSCtz69986
  Symptoms: The Cisco ASR 1000 router’s ESP free memory slowly decreases over time (~ 7MB per day).
  Conditions: This symptom occurs when WCCP is configured on interfaces.
  Workaround: There is no workaround, unless the WCCP interface configuration is removed.

- CSCtz78194
  Symptoms: A Cisco ASR 1000 router that is running Cisco IOS XE Release 3.6 or Cisco IOS Release 15.2(2)S crashes when negotiating multi-SA DVTI in an IPsec key engine process.
  Conditions: This symptom is observed when the Cisco ASR router is configured to receive DVTI multi-SA in aggressive mode and hitting an ISAKMP profile of a length above 31.
  Workaround: Shorten the ISAKMP profile name to less than 31.

- CSCtz80643
  Symptoms: A PPPoE client’s host address is installed in the LNS’s VRF routing table with the `ip vrf receive vrf-name` command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.
  Conditions: This symptom is observed only when the Virtual-access interface is configured with the `ip vrf receive vrf-name` command via the Virtual-Template or RADIUS profile.
  Workaround: There is no workaround.

- CSCtz82711
  Symptoms: Datapath session would
  Conditions: This symptom is observed when SGSN sends echo req before PDP_CREATE_REQ.
  Workaround: There is no workaround.
- **CSCtz85102**
  Symptoms: Packets with the L2 multicast address and L3 unicast address combination could not be forwarded by L2TPv3 tunnel on the Cisco ASR 1000 router.
  Conditions: This symptom is observed with packets with the L2 multicast address and L3 unicast address combination. This issue is seen with all Cisco ASR 1000 series routers.
  Workaround: There is no workaround.

- **CSCtz88716**
  Symptoms: The Xe34_dvti_qos feature is errored out when dividing by zero while executing “expr \{ $actual_rate_data*1.0*$”.
  Conditions: This symptom occurs after active and standby RP ISSU upgrade.
  Workaround: There is no workaround.

- **CSCua10377**
  Symptoms: A Cisco router with Circuit Emulation SPA may suffer an SPA crash.
  Conditions: This symptom occurs when the CE T1 circuit is configured by the end user for AT&T FDL, and the end user transmits FDL messages requesting 4-hour or 24-hour performance statistics.
  Workaround: There is no workaround. If possible, contact the end user and have them reconfigure their device for ANSI FDL.

- **CSCua13418**
  Symptoms: RP-Announce packets are being replicated across all the tunnel interfaces and the count of replication is equal to the number of tunnel interfaces. For example, if there are 3 tunnel interfaces, then each tunnel should forward 1 RP-Announce packet each minute (with the default timer configured). However, in this case, each tunnel is forwarding 3 RP-Announce packets across each tunnel interface. This issue is not specific to the number of interfaces. It can happen with any number of tunnel interfaces.
  Conditions: This symptom is observed when filter-autorp is configured with the `ip multicast boundary` command. This issue is seen on the Cisco 3725 router too, where the incoming packets are being replicated because of the `filter-autorp` command.
  Workaround: Removing filter-autorp resolves the issue. However, you need to remove the `pim` and `boundary` commands first and then reapply the pim and boundary list without the `filter-autorp` keyword. Also, doing this might lead to redesigning of the topology to meet specific requirements.

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

int TuX
ip pim sparse-dense mode
ip multicast boundary XXXXXX
```

- **CSCua27842**
  Symptoms: The Cisco ASR 1000 router crashes in Firewall code due to NULL l4_info pointer. Day 1 issue.
  Conditions: This symptom occurs when the Cisco ASR 1000 router acts as the MPLS L3VPN UHP. It crashes because FW/NAT requires the l4_info to be set. To trigger this issue, the following features must be configured:
  1. MPLS L3VPN (PE).
  2. Zone-Based FW/NAT.
3. MPLS and MP-BGP loadbalance is configured towards the upstream router
   Workaround: There is no workaround.

- CSCua72048
  Symptoms: When configuring “ipv6 vfr max-fragmentation in/out” at no-default value, the ESP
  reloads with traceback.
  Conditions: This symptom is observed when “ipv6 vfr max-fragmentation in/out” is configured at
  no-default value.
  Workaround: There is no workaround.

- CSCua87877
  Symptoms: A crash occurs in ucode.
  Conditions: This symptom is observed with 160cps SIP calls.
  Workaround: There is no workaround.

- CSCua92557
  Symptoms: The active FTP data channel sourced from the outside may not work as expected. Other
  protocol inspections that expect pinhole or door for connections initiated from the outside may be
  affected as well.
  Conditions: This symptom was first identified on the Cisco ASR router running Cisco IOS Release
  15.1(3)S3 with VASI+VRF+PAT+FW. This issue is seen when the FTP client is on the inside and
  the active FTP server is on the outside.
  Workaround: Static NAT will work.

Open Caveats—Cisco IOS XE Release 3.4.3S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.4.3S.

- CSCtr65436
  Symptoms: A Cisco ASR 1000 series router with around 500 spokes starts malfunctioning after it is
  subjected to MOMBA procedures. This symptom is also observed on a Cisco c3945e Integrated
  Services router with around 100 spokes.
  Conditions: This symptom is observed in a dual-hub DMVPN and while switching over between
  hubs.
  Workaround: Do not switch over between hubs.

- CSCts04802
  Symptoms: During vrf transfer, old services are removed but the new service is not applied.
  Conditions: This symptom is observed during a VRF transfer from v1 to v2.
  Workaround: There is no workaround.

- CSCts75470
  Symptoms: Packets do not get intercepted at MD due to multiple ACEs.
  Conditions: This symptom is observed after performing “microcode reload pxf” on IAP and CE1.
  Workaround: Delete the Tap and recreate it.
• CSCtt70133
  Symptoms: The RP resets with FlexVPN configuration.
  Conditions: This symptom is observed when using the clear crypto session command on the console.
  Workaround: There is no workaround.

• CSCtu01601
  Symptoms: A Cisco ASR1000 series router crashes while executing the write memory command.
  Conditions: The conditions that trigger this symptom are not known.
  Workaround: There is no workaround.

• CSCtu35116
  Symptoms: VPDN session keeps on trying to come up with MPLS MTU higher than 1500.
  Conditions: This symptom is observed when you upgrade a Cisco 7200VXR from the c7200-a3jk91s-mz.122-31.SB18 to the c7200-adventerprisek9-mz.122-33.SRE4 image.
  Workaround: There is no workaround.

• CSCtw80678
  Symptoms: Multilink PPP ping fails when the serial interfaces experience QMOVESTUCK error.
  Conditions: This symptom may be observed if multilink PPP member links and serial interfaces on which the QMOVESTUCK error is reported are on the same SPA.
  Workaround: There is no workaround.

• CSCtw98200
  Symptoms: Sessions do not come up while configuring RIP commands that affect the virtual-template interface.
  Conditions: This symptom is observed if a Cisco ASR1000 series router is configured as LNS. RIP is configured with the timers basic 5 20 20 25 command. Also, every interface matching the network statements is automatically configured using the ip rip advertise 5 command. These interfaces include the loopback and virtual-template interfaces too.
  On a Cisco ASR1000 series router, this configuration causes the creation of full VAIIs which are not supported. Hence, the sessions do not come up. On Cisco ISR 7200 routers, VA subinterfaces can be created.
  Workaround: Unconfigure the timers rip command.

• CSCtx11598
  Symptoms: The Router reload causes a Cisco Shared Port Adapter (SPA) failure with the error message “% CWAN_SPA-3-FAILURE: SPA-2CHT3-CE-ATM[2/2]: SPA failure”.
  This can cause the SPA to go to one of the following states:
  - none
  - standby reset
  - down
  And further, this failure leads to unexpected system reload.
  Conditions: This symptom is observed during Router reload for 15-20 times.
  Workaround: Ensure that all the library shared objects are loaded at the time of SPA initialization.
Caveats in Cisco IOS XE 3.4S Releases

OL-23288-23

CSCtx15799
Symptoms: An MTP on a Cisco ASR router sends an “ORC ACK” message through CRC for the channel ID that is just received but does not reply to the ORC for the next channel.
Conditions: This symptom is observed when there is a very short time lapse between the ORC and CRC, say 1 msec.
Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.4.3S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.3S.

CSCee38838
Symptoms: A crashdump may occur during a two-call-per-second load test on a gateway, and the gateway may reload.
Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.3(7)T and that functions as a gateway when you run a two-call-per-second load test that uses H.323, VXML, and HTTP. The crash occurs after approximately 200,000 calls.
Workaround: There is no workaround.

CSCtd86428
Symptoms: SSH session does not accept IPv6 addresses in a VRF interface, but will accept IPv4 addresses.
Conditions: This symptom is observed when you specify the VRF name with an SSH that belongs to an IPv6 interface.
Workaround: You can specify the source interface.
Further Problem Description: SSH sessions do not accept IPv6 addresses in the VRF interface, but accepts IPv4 addresses:
- Telnet session accepts both v6 and v4 addresses in the VRF interface.
- The “Destination unreachable; gateway or host down” message shows in the SSH session to IPv6 addresses in the VRF interface.

CSCtg57657
Symptoms: A router is crashing at dhcp function.
Conditions: This symptom has been seen on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T3.
Workaround: There is no workaround.

CSCti00319
Symptom 1: The warning message “Fatal error FIFO” occurs repeatedly upon PPPoEoA Session teardown.
Symptom 2: On the LC console, the message “Command Indication Q wrapped” keeps appearing.
Conditions: This symptom is observed on a Cisco ASR1001 router and kingpin router chassis under the following conditions:
1. High-scale session counts.
2. Range configuration with more than 100 virtual channels (VC).
3. Back to back creation and deletion of multiple VCs with no time gap.
   Workaround: There is no workaround.

- CSCtj64807
  Symptoms: The router crashes while issuing the `show vlans dot1q internal` command.
  Conditions: This symptom is observed with the following conditions:
  1. One QinQ subinterface configured with inner VLAN as “any”.
  2. More than 32 QinQ subinterfaces configured with same outer VLAN.
  3. All subinterfaces are removed except subinterface configured with “any” inner VLAN.
  Workaround 1: For any Cisco 10000 series router which has had its first crash, on any subinterface if the outer VLAN has second-dot1q VLAN as only “any”, immediately delete the subinterface and recreate it. Then, add a dummy VLAN/sub-interface to this outer VLAN.
  Workaround 2: On any outer VLAN (in array state) if they have less than 5 inner VLANs, add a dummy VLAN/subinterface.
  Workaround 3: For any Cisco 10000 series router which has not had a crash but has subinterface/outer VLAN with second-dot1q VLAN as only “any” and active sessions, add a dummy VLAN/subinterface to this outer (tree state) VLAN.

- CSCtj95685
  Symptoms: A router configured as a voice gateway may crash while processing calls.
  Conditions: This symptom is observed with a router configured as a voice gateway.
  Workaround: There is no workaround.

- CSCtn02372
  Symptoms: QoS installation fails on the CEoP SPA or traffic is not forwarded correctly after a lot of dynamic changes that continuously remove and add VCs, as on CEoP SPA, IfIDs are not freed upon deleting the PVC.
  Conditions: This symptom occurs when continuous bring-up and tear down of VCs causes the SPA to run out of IfIDs.
  Workaround: Reload the Cisco SIP-400 line card.

- CSCtq09712
  Symptoms: A Cisco ASR router’s RP crashes due to L2TP management daemon:
  `%Exception to IOS: Frame pointer 0xXXXXXXXXXXXX, PC = 0xZZZZZZZZZ IOS Thread
  backtrace: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = L2TP mgmt daemon`
  Conditions: This symptom is observed with L2TP when clearing the virtual access interfaces.
  Workaround: There is no workaround.

- CSCtq24557
  Symptoms: The router crashes after deleting multiple VRFs. This happens very rarely.
  Conditions: This symptom is observed in a large-scale scenario.
  Workaround: There is no workaround.

- CSCtq59923
  Symptoms: OSPF routes in RIB point to an interface that is down/down.
Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.

Workaround: Configure “ip routing protocol purge interface”.

- CSCtq77024

Symptoms: Metrics collection fails on hop0 if route change event occurs.

Conditions: This symptom is observed when the mediatrace is not passing up an interface type that is acceptable to DVMC when a route change occurs on the node which has the initiator and responder enabled.

Workaround 1: Remove and reschedule mediatrace session.

Workaround 2: Remove and reconfigure mediatrace responder.

- CSCtq99488

Symptoms: Session is poisoned on standby RP after performing account-logon on native IPv6 session.

Conditions: This symptom is observed upon doing an account-logon on an unauthenticated IPv6 session with L4R applied. The session gets poisoned on the standby. The operation is, however, successful on the active RP.

Workaround: There is no workaround.

- CSCtr47642

Symptoms: On Cisco IOS Release 15.2(3)T that is running BGP configured as RR with multiple eGBP and iBGP nonclients and iBGP RR clients and enabling the BGP best-external feature using the `bgp additional-paths select best-external` command, a specific prefix may not have bestpath calculated for a long time.

Conditions: The problem occurs on a certain condition of configuration of the below commands, and a few prefixes are withdrawn during the configuration time:

1. Configure `bgp additional-paths install` under VPNv4 AF.
2. Configure `bgp additional-paths select best-external`.

Immediately disable backup path calculation/installation using the `no bgp additional-paths install` command.

The problem does not appear if both of the above commands are configured with more than a 10-second delay as the commands will be executed independently in two bestpath runs instead of one.

Workaround: Configure the `bgp additional-paths install` command and the `bgp additional-paths select best-external` command with a delay of 10 seconds.

- CSCtr52740

Symptoms: Query on an SLA SNMP MIB object using an invalid index can cause the device to crash.

Conditions: This symptom is observed when querying history information from `rttMonHistoryCollectionCompletionTime` object using invalid indices.

Workaround: Instead of using “get”, use “getnext” to list valid indices for the MIB OID.
- **CSCtr79905**
  Symptoms: An error message is seen while detaching and reattaching a service policy on an EVC interface.
  Conditions: This symptom is observed when detaching and reattaching the service policy on an EVC interface when port shaper is configured on the interface.
  Workaround: There is no workaround.

- **CSCtr87070**
  Symptoms: Enable login fails with the error “% Error in authentication”.
  Conditions: This symptom is observed with TACACS single-connection.
  Workaround: Remove TACACS single-connection.

- **CSCtr88739**
  Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.
  Symptom 2: The routes in BGP may not get installed to RIB.
  Conditions: These symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 ..... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.
  For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.
  For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.
  Workaround for symptom 1: Remove “import-route target” and reconfigure route-target.
  Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

- **CSCts13474**
  Symptoms: ISSU loadversion fails with the message “Unable to read configuration register”.
  Conditions: This symptom is observed during superpackage ISSU downgrade from Cisco IOS XE Release 3.5 to Cisco IOS XE Release 3.4.
  Workaround: Execute `issu loadversion` again.

- **CSCts15034**
  Symptoms: A crash is seen at dhcpd_forward_request.
  Conditions: This symptom is observed with the DHCP relay feature when it is used with a scaled configuration and significant number of DHCP relay bindings.
  Workaround: If possible, from a functional point of view, remove the `ip dhcp relay information option vpn` command. Otherwise, there is no workaround.

- **CSCts31111**
  Symptoms: Coredump generation fails on the Cisco 800.
  Conditions: This symptom occurs when coredump is configured.
  Workaround: Go to ROMmon, and set a variable WATCHDOG_DISABLE before the coredump happens, as follows:
conf t
config-reg 0x0
end
wr
reload
yes
<rommon prompt>
DISABLE_WATCHDOG=yes
sync
set
conf-reg 0x2102
reset

- **CSCts57108**
  Symptoms: Standby reloads continuously after ISSU RV.
  Conditions: This symptom is observed during a downgrade scenario where the active is running Cisco IOS Release 15.1 and the standby is running Cisco IOS Release 12.2. Cisco IOS Release 15.1 will be syncing the `snmp-server enable traps ipsl` keyword to the standby, but the standby does not understand the new keyword.
  Workaround: Remove references to `snmp-server enable traps ipsl` and then perform the downgrade.

- **CSCts65564**
  Symptoms: In a large-scale DMVPN environment, a DMVPN hub router may crash in the IOS process under high scale conditions.
  Conditions: This symptom only occurs if CRL caching is disabled (with the command `crl cache none` under the pki trustpoint configuration).
  Workaround: Enable CRL caching (this is the configured default).

- **CSCts67465**
  Symptoms: If you configure a frequency greater than the enhanced history interval or if the enhanced history interval is not a multiple of the frequency, the standby will reset.
  Conditions: This symptom is observed always, if the standby is configured as an SSO.
  Workaround: Remove enhanced history interval configuration before resetting the frequency.

- **CSCts70790**
  Symptoms: A Cisco 7600 router ceases to advertise a default route configured via “neighbor default-originate” to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.
  Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.
  Workaround: Remove and readd the `neighbor default-originate` command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- **CSCts71958**
  Symptoms: When the router is reloaded due to crash, the `show version` output shows the reload reason as below:

```plaintext
Last reload reason: Critical software exception, check bootflash:crashinfo_RP_00_00_20110913-144633-PDT
```
After this, the same reason is shown even if the router is reloaded several times using the `reload` command.

Conditions: This symptom is observed after a crash.
Workaround: There is no workaround.

- CSCts97856
Symptoms: PIM Assert is sent out from a router with metric [0/0], though the router has a less preferred path to reach the Source or RP.
Conditions: This symptom occurs when an mroute is first created and its RPF lookup to the Source or RP is via BGP or Static, which involves recursive lookup, or there is no valid path to reach Source or RP. This issue only occurs in a small window in milliseconds. After the window, the metric [0/0] is corrected.
Workaround: There is no workaround.

- CSCts97925
Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.
Conditions: This symptom is observed only with IPv6, and not with IPv4.
Workaround: Disable IPv6 CEF.

- CSCtt02313
Symptoms: When a border router (BR) having a parent route in EIGRP is selected, "Exit Mismatch" is seen. After the RIB-MISMATCH code was integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.
Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.
Workaround: There is no workaround.

- CSCtt17785
Symptoms: In the output of `show ip eigrp nei det`, a Cisco ASR router reports peer version for Cisco ASA devices as 0.0/0.0. Also, the Cisco ASR router does not learn any EIGRP routes redistributed on the Cisco ASA device.
Conditions: This symptom is observed only when a Cisco ASR router is running on Cisco IOS Release 15.1(3)S and the Cisco ASA device is Cisco ASA Version 8.4(2).
Workaround: Downgrade the Cisco ASR router to Cisco IOS Release 15.1(2)S.

- CSCtt17879
Symptoms: The `bgp network backdoor` command does not have any effect.
Conditions: This symptom occurs:
- On 64-bit platform systems.
- When the network is learned after the backdoor has been configured.
Workaround: Unconfigure and reconfigure the network backdoor.

- CSCtt26074
Symptoms: Memory leak with IP SLAs XOS Even process.
Conditions: This symptom is observed with IP SLA configured.
Workaround: There is no workaround.
• CSCtt37516
Symptoms: Line card crash with priority traffic when QoS policy is applied.
Conditions: This symptom is observed with the QoS priority feature.
Workaround: There is no workaround.

• CSCtt43843
Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.
Conditions: This symptom is occurring with a Cisco 7200 platform that is loaded with the Cisco IOS Interim Release 15.2(1.14)T0.1 image.
Workaround: There is no workaround.

• CSCtt53985
Symptoms: All traffic stops forwarding on a Cisco ASR 1000 series router due to the ESP crashing. Or, half entries with the IP address 239.67.33.205 may show up in the database, which may cause some end stations to be improperly translated. Or, with dynamic configurations two sessions could have the same inside global, but different inside locals (happens very rarely). The workaround for this last condition is to clear the offending session.
Conditions: This symptom is observed in a rare condition that can result in an ESP crash or bad half entry translations as described above.
Workaround: For the crash, prevent SNMP from pulling NAT OIDs. This only works sometimes. An upgrade is the best recommended action. This can be done by creating a view. For example:
```
snmp-server view test internet included snmp-server view test 1.3.6.1.4.1.9.10.77.1 excluded snmp-server community pub view test RO
```
To recover from the bad entries, a reload is required.

• CSCtu00699
Symptoms: On a DMVPN hub router, the IOS processor memory pool can get fragmented due to memory allocated for “Crypto NAS Port ID”.
Conditions: This happens when there is network instability potentially causing tunnels to flap frequently.
Workaround: There is no workaround.

• CSCtu13951
Symptoms: Pending objects appear on the active and standby ESP.
Conditions: This symptom occurs when the edge device to the core link is flapped multiple times for close to two days.
Workaround: There is no workaround.

• CSCtu20929
Symptoms: Primary path is disabled when FRR is triggered by a SPA OIR.
Conditions: This symptom occurs due to a functionality issue and is seen when the primary path and backup path are in different SPAs. The impact is that OSPF is stuck in an INIT state and traffic flow is affected.
Workaround: Reload the SPA.

• CSCtu24460
Symptoms: A Cisco ASR 1000 router crashes.
Conditions: This symptom is observed on a Cisco ASR 1000 router that is configured as LNS with per subscriber firewall. Releases affected by this defect: Cisco IOS Release 15.1(3)S, 15.1(3)S1, 15.1(3)S2, and 15.2(1)S.

Workaround: There is no workaround to this issue. Configuring firewall TCP and UDP timers lower than 1200 seconds may reduce the probability of the crash.

- CSCtu28990
  Symptoms: RP crash is observed at SYS-6-STACKLOW: Stack for process XDR Mcast.
  Conditions: This symptom is observed when performing shut/no shut on interfaces on a configuration-rich system.
  Workaround: There is no workaround.

- CSCtu32301
  Symptoms: Memory leak may be seen.
  Conditions: This symptom is seen when running large show commands like `show tech-support` on the line card via the RP console.
  Workaround: Do not run the show commands frequently.

- CSCtu38244
  Symptoms: After bootup, the GM cannot register and is stuck in "registering" state. Issuing the `clear crypto gdoi` command is required for a successful registration to the keyserver.
  Conditions: This symptom is observed upon router bootup.
  Workaround: Either do a clear crypto gdoi after a reload, or configure a second keyserver entry. This does not have to be an existing keyserver, it can be just a dummy address.

- CSCtu39819
  Symptoms: The Cisco ASR 1002 router configured as an RSVPAgent for Cisco Unified Communication Manager crashes under extended traffic.
  Conditions: This symptom is observed on a Cisco ASR 1002 router configured as an RSVPAgent for CUCM End-to-End RSVP feature. The router crashes after 45 minutes of traffic run with 150 simultaneous up MTP-RSVP sessions.
  The image used is “asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin”.
  Workaround: There is no workaround.

- CSCtu41137
  Symptoms: IOSD Core@fib_table_find_exact_match is seen while unconfiguring tunnel interface.
  Conditions: This symptom is observed while doing unconfiguration.
  Workaround: There is no workaround.

- CSCtu98960
  Symptoms: The QL value is DNU although the four least significant bits of SSM S1 byte are pointing to PRC (bits: 0010).
Conditions: This symptom is observed when SSM S1 byte is received on CEoPs SPAs or channelized SPA-1XCHSTM1/OC3.

Workaround: Force the QL PRC value by executing the following command:

```
network-clock quality-level rx QL-PRC controller SONET 1/2/0
```

**CSCtw48209**

Symptoms: High-end Cisco devices running Cisco IOS are likely affected. Active features at the time of this problem manifestation include any condition that leads to RSVP SNMP notification generation in Cisco IOS. BGP/MPLS TE instability, leading to changes to RSVP session status change, is observed in a test scenario while running Cisco IOS Release SXI4 and Cisco IOS Release SXI7. The issue is not reproducible consistently.

Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SXI4, Cisco IOS Release 12.2(33)SXI7, Cisco IOS Release 12.2SR, Cisco IOS Release 12.2SX, and Cisco IOS Release 15S.

Workaround: Disable RSVP notification using the `no snmp-server enable traps rsvp` command.

**CSCtw52610**

Symptoms: Some of the TCes will switch to fallback interface, and the remaining TCes on primary interface will be in OOP state.

Conditions: This symptom is observed when the primary link is considered OOP based on utilization despite using the `no resolve utilization` command.

Workaround: There is no workaround if PfR policy with and without utilization is needed. If PfR policy based on utilization is not needed, then configure "max-xmit-utilization percentage 100".

**CSCtw56012**

Symptoms: On a Cisco ASR 1000 series Asynchronous Object Manager (AOM), pending-ack objects may be seen after removing an ATM multipoint subinterface configured on a SPA-2CHT3-CE-ATM (T3 or E3 mode). This prevents subsequent configuration updates on the same subinterface, resulting in a traffic drop on the PVCs configured under that subinterface.

Conditions: This symptom occurs when a multipoint ATM subinterface is deleted on a SPA-2CHT3-CE-ATM (T3 or E3 mode).

Workaround: Use a different subinterface if a reconfiguration of the same PVP and/or PVC is required. For example, the original configuration is:

```
! interface ATM0/0/1.2000 multipoint
ip address 10.3.2.1 255.255.255.0
atm pvp 200
no atm enable-ilmi-trap
pvc 200/100
protocol ip 10.3.2.2 broadcast
protocol ip 10.3.2.3 broadcast
encapsulation aal5snap
!
end
```

and subinterface ATM0/0/1.2000 was deleted resulting in a pending-ack on the subinterface. Then, to reconfigure the same PVP or PVC, use a different number (ATM0/0/1.2001) for the subinterface:

```
! interface ATM0/0/1.2001 multipoint
ip address 10.3.2.1 255.255.255.0
atm pvp 200
no atm enable-ilmi-trap
pvc 200/100
```
Further Problem Description: When this problem occurs, the AOM pending-ack objects correspond to the deleted multipoint subinterface as shown in the example below:

```plaintext
Router#show platform software object-manager fp active statistics
Forwarding Manager Asynchronous Object Manager Statistics
Object update: Pending-issue: 0, Pending-acknowledgement: 1
Batch begin: Pending-issue: 0, Pending-acknowledgement: 0
Batch end: Pending-issue: 0, Pending-acknowledgement: 0
Command: Pending-acknowledgement: 0
Command: Stale-objects: 0

Router#show platform software object-manager fp active pending-ack-update
Update identifier: 269
Object identifier: 358
Description: intf ATM0/0/1.2000, handle 44, hw handle 46,
dirty 0x0, AOM dirty 0x0
Number of retries: 0
Number of batch begin retries: 0

Router#show platform software object-manager fp active object 358
Object identifier: 358
Description: intf ATM0/0/1.2000, handle 44, hw handle 46,
dirty 0x0, AOM dirty 0x0
Status: Pending-acknowledgement, Epoch: 0, Client data: 0x1171aac0

Issued action
Update identifier: 269, Batch identifier: 0
Batch type: unknown
Action: Delete
```

Note that this problem is not seen when a point-to-point ATM subinterface is deleted on a SPA-2CHT3-CE-ATM (T3 or E3 mode). It is also not seen on point-to-point, or multipoint ATM subinterfaces on SPA-1XOC3-ATM-V2, SPA-3XOC3-ATM-V2, and SPA-1XOC12-ATM-V2 SPAs.

- CSCtw56439
  Symptoms: The **ip mtu** command that is configured on an IPsec tunnel disappears after a router reload.
  Conditions: This symptom is observed with IPsec and the **ip mtu** over a tunnel interface.
  Workaround: There is no workaround.

- CSCtw62310
  Symptoms: The **cells** keyword is added to “random-detect” whenever a policy-map is removed from an interface/map-class via “no service-policy”.
  Conditions: This symptom is observed when removing the policy-map from map-class.
  Workaround: There is no workaround.

Further Problem Description: The CLI is technically valid if it has been manually configured as “cells” prior to the removal. The issue is that the template policy is being changed automatically to “cells” whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.
CSCtw69820
Symptoms: A router with Zone Based Firewall (ZBFW) enabled allows dest.port 0 packets by default. If such packets arrive at a high rate, performance issues may be seen to the extent that OSPF/BGP/EIGRP sessions are dropped, along with high latency on data traffic.
Conditions: This symptom is observed if ZBFW is enabled and there is TCP/UDP traffic with dest.port 0.
Workaround: Deny dest.port 0 packets in the ZBFW policy.

CSCtw71564
Symptoms: Not all data packets are accounted for in the show stats command output of the video operation.
Conditions: This symptom is observed with heavy load on the responder caused either by many video sessions or other processes.
Workaround: Reduce processor load on device running the responder.

CSCtw76044
Symptoms: IGMP/MLD information is needed to make IGMP/MLP snooping work.
Conditions: This symptom is observed under all conditions.
Workaround: There is no workaround.

CSCtw78451
Symptoms: A Cisco ASR 1000 series router may reload when multiple users are logged in running show commands.
Conditions: This symptom is only seen when the Cisco ASR router is used as a DMVPN headend and there are hundreds of tunnels flapping.
Workaround: There is no workaround. However, this appears to be a timing issue when there is instability in a large-scale environment.

CSCtw88094
Symptoms: The standby management processor reloads during configuration sync when there is a mismatch in the IP SLA configuration.
Conditions: This symptom occurs shortly after the ip sla schedule X start specific_start_time command is issued multiple times on the same probe instance. Hence, when the configuration is synced to the standby management processor, a PRC error occurs. The PRC error causes a reload of the standby management processor.
Workaround: Unschedule the probe before rescheduling for a specific start time.

CSCtw94319
Symptoms: A crash is seen at dhcpd_forward_request.
Conditions: This symptom is seen when the IP DHCP Relay feature is used in scaled configuration.
Workaround: Remove the ip dhcp relay information option vpn command, if possible. Otherwise, there is no workaround.

CSCtw94598
Symptoms: Web authentication does not work after an upgrade. NAS-Port-Type = Async.
Conditions: This symptom is observed when you upgrade to Cisco IOS Release 12.2 (58)SE2 or later or to the Cisco IOS 15.0(1)SE train.
Workaround: Change NAS-Port-Type on the AAA server to match the new value.
- **CSCtw98456**
  Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK but no traffic is going out over the tunnel.

  Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).

  For example, the IVRF routing table should show:
  
  S 10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1

  but instead it shows:
  
  S 10.0.0.0 [1/0] via 192.168.0.1

  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

  Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in `show crypto ipsec sa`) remain at zero.

  Conditions: This has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other IOS versions and other hardware platforms may be affected.

  Workaround: Configure a static route to the remote network. For example:
  
  ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1

  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- **CSCtw99290**
  Symptoms: The source or destination group-address gets replaced by another valid group-address.

  Conditions: This symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

  Workaround: There is no workaround.

- **CSCtw99989**
  Symptoms: The source or destination group-address gets replaced by another valid group-address.

  Conditions: This symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

  Workaround: There is no workaround.

- **CSCtx01370**
  Symptoms: Multicast convergence can be seen in NATted environment for a dual homed Cisco ASR 1000 router CPE running 3.4.1 code (primary and secondary CPE) connecting to different PEs, although multicast traffic is not NATted. The convergence reported in the issue is approximately two minutes.
Conditions: This symptom is observed on a Cisco ASR 1000 router CPE running 3.4.1 code (primary and secondary CPE) connecting to different PEs.

Workaround: The workaround is to prevent RPT to SPT switchover by configuring “ip pim spt-threshold infinity”.

Further Problem Description: The issue is caused by out of order PIM messages send during convergence resulting in outgoing interface on secondary CPE as null.

- CSCtx01604
  Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.
  Conditions: This symptom presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.
  Workaround: Do not use any dynamic network interface IP address as CNS ID.

- CSCtx21547
  Symptoms: Ucode and fman-fp crash.
  Conditions: This symptom is observed with a firewall configuration/unconfiguration with HSL configuration in “global inspect parameter-map” after unconfiguring the firewall.
  Workaround: Remove the HSL configuration in “global inspect parameter-map” before unconfiguring the firewall, that is, remove the following configuration: “log flow-export v9 udp destination <IP> <Port>” from “parameter-map type inspect global” or from “parameter-map type inspect- global”.

- CSCtx28483
  Symptoms: A router set up for Cisco Unified Border Element-Enterprise (CUBE-Ent) box-to-box redundancy reloads when certain configuration commands are deconfigured out of the recommended sequence.
  Conditions: This symptom is observed when deconfiguring CUBE-Ent box-to-box redundancy once it is already configured (for CUBE-Ent box-to-box redundancy) on the Cisco ASR platform. You cannot change the configuration under the “application redundancy group” submode without first removing the redundancy-group association under “voice service voip” submode. If you do not remove this association first before changing the configuration under “application redundancy group”, the ASR will reload. You are not provided any other option.
  Workaround: Always first remove the redundancy-group association under “voice service voip” submode first and then you can change the configuration under “application redundancy group”.

- CSCtx29543
  Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the show ip route command.
  Conditions: This symptom occurs under the following conditions:
  1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exist.
  2. A default route exists.
  3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.
  The router may now crash when doing show ip route command or when the default route is updated.
  Workaround: There are two possible workarounds:
  1. Ensure that not all 23 supernet mask lengths are populated by doing route filtering.
2. If workaround #1 is not possible, then ensure that at least one supernet route for all possible mask lengths exists at all times, for example, by configuring summary routes that do not interfere with normal operation.

- CSCtx29557
  Symptoms: A standby crashes at fib_fib_src_interface_sb_init.
  Conditions: This symptom is observed with fib_fib_src_interface_sb_init.
  Workaround: There is no workaround.

- CSCtx31175
  Symptoms: Framed-IP-Address added twice in PPP service-stop accounting record.
  Conditions: This symptom is observed with the following conditions:
  1. User session exists on ASR1001.
  2. Stop one user’s session by using clear subscriber session username xxx on the Cisco ASR 1001 router.
  3. The Cisco ASR 1001 router sends double “Framed-IP-Address” in service-stop accounting for one user’s session.
  Workaround: Do not use the clear subscriber session command to clear the session; instead, use clear pppoe.

- CSCtx32628
  Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.
  Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:
  - BGP full mesh is configured.
  - BGP cluster-id is configured.
  - address family vpnv4 is enabled.
  - address family ipv4 mdt is enabled.
  - The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.
  Workaround: Remove the cluster-id configuration or hard-reset the bgp session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

- CSCtx35463
  Symptoms: Output is truncated.
  Conditions: This symptom is observed when displaying show platform hardware qfp act feature nat data ha.
  Workaround: There is no workaround.

- CSCtx35498
  Symptoms: ASRNAT B2B: sessions are not aged on the active.
  Conditions: This symptom occurs when the standby stays down.
  Workaround: Do not have the standby down for extended time periods.
• CSCtx35692

Symptoms: On the Cisco ASR 1000 platform, while acting in a redundancy pair, when the standby ASR becomes active the dial-peers on the standby never change their state back to active causing all calls to fail. Calls that were active during the failover scenario will stay active in the new switchover. Only new calls are affected.

Conditions: This symptom is observed on an ASR 1000 series router CUBE with a box-to-box redundancy configured that is using OOD option pings in the dial-peers. Global configuration of option pings under voice service VoIP is only for IN-Dialog option pings.

Workaround: Disable option keepalives from the dial-peers.

• CSCtx37240

Symptoms: AOM pending-ack objects are seen on Tx Channels of Serial interfaces after router reload.

Conditions: This symptom is observed with scale setup with hundreds of (channelized) serial interfaces present in the configuration. Reload the router with this configuration.

Workaround: There is no workaround.

• CSCtx47213

Symptoms: The following symptoms are observed:

1. Session flap when iBGP local-as is being used on RR.
2. Replace-as knob is not working in iBGP local-as case.

Conditions: This symptom is observed with the following conditions:

1. The session will flap when iBGP local-as is used on the RR client and RR sends an update.
2. Replace-as knob even used is ignored and prefixes are appended with local-as.

Workaround: Do not use iBGP local-as.

• CSCtx51935

Symptoms: Router crashes after configuring “mpls traffic-eng tunnels”.

Conditions: This symptom is observed with the following steps:

```plaintext
interface gi1/2
mpls traffic-eng tunnels
no shut

router OSPF 1
mpls traffic-eng area 100
mpls traffic-eng router-id lo0
end

show mpls traffic-eng link-management summary
```

Workaround: There is no workaround.

• CSCtx55357

Symptoms: Auto RP messages are permitted through “ip multicast boundary”.

Conditions: This symptom is observed when the ACL associated with the multicast boundary matches 224.0.1.39 and 224.0.1.40. It is seen on the Cisco ASR 1000 platform.

Workaround: Use “no ip pim autorp” which will disable Auto RP completely from this device.
- **CSCtx67474**
  Symptoms: An update message is sent with an empty NLRI when the message consists of 2byte aspath in ASPATH attribute and 4byte value aggregate attribute.
  Conditions: This symptom can occur when there is a mix of 2byte and 4byte attributes in the update message and the message is sent from a 2byte peer and there is a 4byte aggregator attribute.
  Workaround: Move all the 2byte AS peers to a separate update-group using a non-impacting outbound policy like “advertisement-interval”.

- **CSCtx70505**
  Symptoms: Standby FP crashes and gets stuck in INIT standby state after an FP restart.
  Conditions: This symptom is observed with BBA client login and logout with high TPS. Run `sh platform software peer chassis-manager fp standby` periodically.
  Workaround: Reload the router.

- **CSCtx71618**
  Symptoms: The router crashes at process L2TP mgmt daemon.
  Conditions: This symptom is observed with a Cisco ASR 1006 (RP2) running Cisco IOS Release 15.1(2)S.
  Workaround: There is no workaround.

- **CSCtx73452**
  Symptoms: The following symptoms are observed:
  1. You send an ICMPv4 packet with IP option. It will be forwarded by the Cisco ASR1001 router. The IP options field includes the “loose source routing” option.
  2. The Cisco ASR 1001 router receives the packet. The Cisco ASR 1001 router has “no ip source-route” setting in its configuration.
  3. The Cisco ASR 1001 router incorrectly overwrites the destination IP address of packet, which has source-route option set, and forwards it instead of dropping it.
  Conditions: This symptom is observed with the Cisco ASR 1001 (2.5G ESP).
  Workaround: There is no workaround.

- **CSCtx73612**
  Symptoms: A Cisco ASR 1000 router may reload while reading IPsec MIBs via SNMP and write a crashfile.
  Conditions: This symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.1(1)S1.
  Workaround: Do not poll or trap IPsec information via SNMP.

- **CSCtx82775**
  Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.
  Conditions: This symptom is observed when MTP is invoked for calls.
  Workaround: Reload the router or perform a no sccp/sccp.

- **CSCtx86069**
  Symptoms: The dynamic NAT has a wrong translation that causes multiple inside local addresses to be translated to the same inside global address.
  Conditions: This symptom is observed with the following conditions:
- Cisco IOS XE Release 3.4.2.
- Call flow: multiple sip caller -- proxy --(inside)-- ALG --(outside)-- sip callee.
- Inside dynamic NAT is configured, with one hour timeout.

Steps of reproducing:
1. Make some of the SIPP calls for several hours.
2. After some hours, make calls from idle SIPP.

For the new inside local IP address, NAT will be translated to an existing inside global in the table (without create a new binding in NAT table), which is bound with another inside local address.

Workaround: There is no workaround.

• CSCtx96285
Symptoms: A configuration of stateful inter-chassis redundancy for NAT may result in packets routing through the standby router and not being processed by the NAT rules, or dropped (NAT is being bypassed).

Conditions: This symptom is observed after a failover of primary to secondary with all routing protocols forcing traffic to the standby router.

Workaround: There is no workaround.

• CSCtx99544
Symptoms: Exception occurs when using `no aaa accounting system default vrf VRF3 start-stop group RADIUS-SG-VRF3`:

```
router(config)# no ip vrf VRF3
router(config)# no aaa accounting system default vrf VRF3 start-stop group RADIUS-SG-VRF3
```

%Software-forced reload

Conditions: This symptom is observed with the following conditions:
- Hardware: Cisco ASR 1001.

Workaround: There is no workaround.

• CSCty02403
Symptoms: EIGRP topo entry with bogus next-hop is created when more than one attribute is present in the route received from neighbors. It also tries to install one default route with bogus next-hop. So if you have a default route received from some neighbors, then that default route will also be flapped.

Conditions: This symptom can only occur when you have more then one attribute set in any route received from a neighbor.

Workaround: Do not set more then one attribute in the route.

• CSCty17747
Symptoms: On a Cisco ASR 1000 router that contains an ESP40 forwarding card or on a Cisco ASR 1001 router, there is an issue that prevents Traditional Netflow (TNF) exporters configured under the aggregation cache command from being properly created when the router is reloaded and booted from the startup configuration. A typical command snippet would look like:

```
ip flow-aggregation
  cache prefix
```
cache entries 512000
cache timeout active 5
export version 9
export template refresh-rate 5
export destination 192.168.1.2 9995
export destination 192.168.3.4 9995
mask source minimum 32
mask destination minimum 32
enabled
!

If this configuration is in the startup-configuration and the router is reloaded, the exporter commands will not take effect after the reload and no packets will be exported.

Conditions: This defect has only been observed on either ESP40 forwarding cards or on a Cisco ASR 1001 router. This defect does not occur during manual configuration but only when the router is reloaded and the startup-configuration (or other bootup configuration) is parsed.

Workaround: Reapply the missing exporter configuration manually after the router is already up.

- CSCty37445
  Symptoms: A DMVPN hub router with a spoke which is an EIGRP neighbor. The spoke receives a subnet from hub and then advertises it back to the hub, bypassing split horizon.
  Conditions: This symptom is observed when on the spoke you have a `distribute list route-map` command setting tags.
  Workaround: Once you remove that command EIGRP works normally.

- CSCty41067
  Symptoms: The router crashes while doing an SSO without any configurations.
  Conditions: This symptom is observed while doing an SSO.
  Workaround: There is no workaround.

- CSCty46022
  Symptoms: A Cisco ASR 1000 router experiences high ESP CPU constantly.
  Conditions: This symptom is observed when ISG sessions with DHCP initiator are experiencing fragmented traffic and the fragmented traffic has a small packet size. The packets will be punted to ESP CPU and cause it to be busy.
  Workaround: There is no workaround.

**Open Caveats—Cisco IOS XE Release 3.4.2S**

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.4.2S.

- CSCtw45055
  Symptom: A Cisco ASR router may experience a crash in the BGP Scheduler due to a segmentation fault if BGP dynamic neighbors have been recently deleted due to link flap. For example:

```
Nov 10 08:09:00.238: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
Nov 10 08:10:20.944: %BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold time expired) x bytes
Nov 10 08:10:20.944: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification received
Nov 10 08:10:20.945: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from session Neighbor deleted
```
Caveats in Cisco IOS XE 3.4S Releases

OL-23288-23

Nov 10 08:10:34.328: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from session Neighbor deleted
Nov 10 08:10:51.816: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up

Exception to IOS Thread:
Frame pointer 0x3BE784F8, PC = 0x104109AC

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler
The scheduler process will attempt to reference a freed data structure, causing the system to crash.

Conditions: This symptom is observed when the Cisco ASR router experiences recent neighborship removals, either because of flapping or potentially by manual removal.

Workaround: There is no workaround.

- CSCtu20223
  Symptoms: An unexplained change is observed in the MTU value written in the running configuration.
  Conditions: This symptom is observed with a Cisco ASR 1002 router running Cisco IOS Release 15.1(2)S1.
  Workaround: There is no workaround.

- CSCtw69820
  Symptoms: A router with Zone Based Firewall (ZBFW) enabled allows dest.port 0 packets by default. If such packets arrive at a high rate, performance issues may be seen to the extent that OSPF/BGP/EIGRP sessions are dropped, along with high latency on data traffic.
  Conditions: This symptom is observed if ZBFW is enabled and there is TCP/UDP traffic with dest.port 0.
  Workaround: Deny dest.port 0 packets in the ZBFW policy.

- CSCtw48209
  Symptoms: High-end Cisco devices running Cisco IOS are likely affected. Active features at the time of this problem manifestation include any condition that leads to RSVP SNMP notification generation in Cisco IOS. BGP/MPLS TE instability, leading to changes to RSVP session status change, is observed in a test scenario while running Cisco IOS Release SXI4 and Cisco IOS SXI7. The issue is not reproducible consistently.
  Conditions: This symptom is observed with Cisco IOS Release SXI4, Cisco IOS Release SXI7, Cisco IOS SR Release, Cisco IOS SX Release, and Cisco IOS S Release.
  Workaround: Disable RSVP notification using the no snmp-server enable traps rsvp command.

- CSCtu31099
  Symptoms: A crash related to VRRP occurs.
  Conditions: This symptom is observed with VRRP. This issue may be also accompanied with the following error message. Also, if repeated Duplicate address messages are seen, it is because of a misconfiguration.
  %IP-4-DUPADDR: Duplicate address X.X.X.X on [Interface], sourced by [MAC-Address]

  Workaround: Use HSRP. If you are currently using owner mode for your configuration, all you need to do is assign a single unique address to the "owner mode" interface so that it does not match the virtual address. Then, assign a high priority to HSRP on this interface, and you will have an equally functionality to before. The only valid reason for not using HSRP would be if you need to operate with another vendor's equipment.

  For example:
int e0/0
ip address 172.24.1.1 255.255.255.0
vrrp 1 ip 172.24.1.1

Just needs to be changed to:

int e0/0
ip address 172.24.1.42 255.255.255.0
standby 1 ip 172.24.1.1
standby 1 priority 254

CSCtg57657
Symptoms: A router crashes at the DHCP function.
Conditions: This symptom is observed on a Cisco 7206VXR router running Cisco IOS Release 12.4(22)T3.
Workaround: There is no workaround.

CSCts97856
Symptoms: PIM Assert is sent out from a router with metric [0/0], though the router has a less preferred path to reach the Source or RP.
Conditions: This symptom occurs when an mroute is first created and its RPF lookup to the Source or RP is via BGP or Static, which involves recursive lookup, or there is no valid path to reach Source or RP. This issue only occurs in a small window in milliseconds. After the window, the metric [0/0] is corrected.
Workaround: There is no workaround.

CSCtt53985
Symptoms: All traffic stops forwarding on a Cisco ASR 1000 series router due to the ESP crashing. Or, half entries with the IP address 239.67.33.205 may show up in the database, which may cause some end stations to be improperly translated.
Conditions: This symptom is observed in a rare condition that can result in an ESP crash or bad half entry translations as described above.
Workaround: For the crash, prevent SNMP from pulling NAT OIDs. This can be done by creating a view. For example:

```
    snmp-server view test internet included
    snmp-server view test 1.3.6.1.4.1.9.10.77.1 excluded
    snmp-server community pub view test RO
```
To recover from the bad entries, a reload is required.

CSCtw74100
Symptoms: An issue with the PPP interface is seen upon flapping the core interfaces.
Conditions: This symptom is observed when shut/no shut on the core interfaces is done through a script overnight, leading to a few PPP serial interfaces going up/down.
Workaround: Shut/no shut on the serial interface resolves the issue.

CSCtw78451
Symptoms: A Cisco ASR 1000 series router may reload when multiple users are logged in running show commands.
Conditions: This symptom is only seen when the Cisco ASR router is used as a DMVPN headend and there are hundreds of tunnels flapping.
Workaround: There is no workaround. However, this appears to be a timing issue when there is instability in a large-scale environment.

Resolved Caveats—Cisco IOS XE Release 3.4.2S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.2S.

- **CSCsg48725**
  
  **Symptoms:** A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:
  
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  
  **Conditions:** This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.
  
  **Workaround:** Disable AAA. If this not an option, there is no workaround.
  
  **Additional Note:** This bug is fixed in Cisco IOS Release 12.2(28)SB7 via CSCsa40461.

- **CSCsh39289**
  
  **Symptoms:** A router may crash under a certain specific set of events.
  
  **Conditions:** The crash may happen under a combination of unlikely events when an IPv6 PIM neighbor that is an assert winner expires.
  
  **Workaround:** There is no obvious workaround, but the problem is unlikely to occur.

- **CSCta27728**
  
  **Symptoms:** A Cisco router may crash.
  
  **Conditions:** This symptom is observed on a Cisco ASR1002 router running Cisco IOS Release 15.1(2)S1 with RSVP for MPLS TE tunnel signaling.
  
  **Workaround:** There is no workaround.

- **CSCtc96631**
  
  **Symptoms:** Packet drops occur in downstream devices every 4ms burst from shaper.
  
  **Conditions:** This symptom is observed when shaping at high rates on very fast interface types with low memory buffer devices downstream.
  
  **Workaround:** Use ASRs instead of ISR.

- **CSCti33159**
  
  **Symptoms:** The PBR topology sometimes chooses a one-hop neighbor to reach a border, as opposed to using the directly-connected link.
  
  **Conditions:** This is seen when the border has multiple internal interfaces and one of the internal interfaces is directly connected to a neighbor and the other interface is one hop away.
  
  **Workaround:** There is no workaround.

- **CSCtj30238**
  
  **Symptoms:** WRED counters are wrongly updated. The default counter should be 0, but the counter is wrongly updated. All the WRED subclasses show the same count. Counters are shown for WRED subclasses for which there are no traffic matches in the class.
Conditions: This symptom is observed on the Cisco 7600 router with ES+ line card only. The ES+ line card does not support per WRED class-based counters. There was a recent breakage due to the Transmit packets/bytes column that started showing up for the ES+ line card. This is wrong. As ES+ writes the same value to the WRED transmit count (not the per subclass base count, but total count), this value does not make sense.

Workaroud: Do not use WRED subclass Transmit packets/bytes counters for ES+ line card on the Cisco 7600 router.

- CSCtk62763
  Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.
  Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.
  Workaroud: There is no workaround.

- CSCtl50815
  Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:

  %OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>,
  Reason Non-OER, OOP Reason <reason>

  Conditions: This symptom is observed under the following conditions:
  - Use ECMP.
  - Use mode monitor passive.
  Workaroud: Remove equal cost routing. For instance, in a situation where you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly as necessary.

  Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl83517
  Symptoms: The last switchover redundancy mode shows the configured mode.
  Conditions: This symptom occurs if DIVC ISSU results puts the system in RPR mode, and the last switchover redundancy mode still shows SSO. When a system tries to come out of RPR to SSO through either manual reset of standby or OIR, it will be stuck in RPR and will not progress to SSO as the last switchover flag shows SSO, and clients assume it is already in SSO.
  Workaroud: There is no workaround.

- CSCtn07696
  Symptoms: The Cisco 6506-E/SUP720 may crash while redirecting the show tech-support command output using the ftp command due to TCP-2-INVALIDTCB.
  Conditions: This symptom is observed with the following CLI:

  `show tech-support | redirect
tftp://cisco@cisco@10.0.255.14/Cisco/tech-support_swan21.pl.txt`

  During the FTP operation, if the interface fails or shuts down, it could trigger this crash.
Workaround: This is an FTP-specific issue. Redirect the output by TFTP or other protocols.

- CSCtn59075
  Symptoms: A router may crash.
  Conditions: This has been experienced on a Cisco router that is running Cisco IOS Release 15.1(3)T, Cisco IOS Release 15.1(3)T1, and Cisco IOS Release 15.1(4)M. Flexible NetFlow needs to be running.
  Workaround: Disable Flexible NetFlow on all interfaces.

- CSCto71671
  Symptoms: Using the `radius-server source-ports extended` command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.
  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.
  Workaround: There is no workaround.

- CSCto81701
  Symptoms: The PfR MC and BR sessions flap.
  Conditions: This symptom is observed with a scale of more than 800 learned TCs.
  Workaround: Use the following configuration:
  ```
  pfr master
  keepalive 1000
  ```

- CSCto88393
  Symptoms: CPU hogs are observed on a master controller:
  `%SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (0/0), process = OER Master Controller.`
  Conditions: This symptom is observed when the master controller is configured to learn 10,000 prefixes per learn cycle.
  Workaround: There is no workaround.

- CSCtq29547
  Symptoms: The router crashes on watchdog timeout while processing the SNMP request for ciscoEigrpMIB.
  Conditions: This symptom occurs while processing the SNMP request for ciscoEigrpMIB.
  Workaround: Exclude ciscoEigrpMIB from being polled by using the following SNMP view:
  ```
  snmp-server view NOCRASH internet included
  snmp-server view NOCRASH ciscoEigrpMIB excluded
  ```
  Then, apply the view to your SNMP community string:
  ```
  snmp-server community test view NOCRASH
  ```

- CSCtq49325
  Symptoms: A router reloads when a graceful shutdown is done on EIGRP.
  Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.
Workaround: Redundant LANs may not be necessary in the first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shut down completely before executing the second shutdown command. This should resolve the problem.

Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other, causing this zombie entry creation for the query also. In the query function flow, it is expected that this zombie entry will not be deleted immediately; rather it is to be deleted only after a reply for the query is sent successfully. At this point, (that is, before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. However, if a particular path is threaded to be sent, in this case, it is scheduled for a reply message, the path is not deleted and an error message is printed. However, the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now, when the neighbors are deleted, the flushing of the packets to be sent will lead to a crash as it does not find the prefix corresponding to the path. The solution is to unthread from the paths from sending before deletion. A similar condition will occur if the packetization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- CSCtq60703
  Symptoms: The device crashes and traceback is seen when executing the `write network` command.
  Conditions: This symptom is observed when the `write network` command is used with no URL specified.
  Workaround: Specify a URL.

- CSCtq61128
  Symptoms: The router crashes with Segmentation fault (11).
  Conditions: This symptom is observed on routers acting as the IPsec hub using certificates.
  Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2:


CVE ID CVE-2011-4231 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:


- CSCtq88777
  Symptoms: The VDSL controller and ATM interface remains up; however, ATM PVC becomes inactive and virtual interface goes down.
  Conditions: This symptom is observed when the ATM PVC becomes inactive, causing the virtual interface to go down.
  Workaround: Use a VBR-NRT value that is lower than the trained upstream speed.

- CSCtq92940
  Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.
Conditions: This symptom may be seen when an active FTP connection is used (that is, the `no ip ftp passive` command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.

Workaround: Use passive FTP (default) by configuring the `ip ftp passive` command.

Further Problem Description: Please see the original bug (CSCtl19967) for more information.

- **CSCtr04829**
  Symptoms: A device configured with “ip helper-address” drops packets because of a zero hardware address check.
  Conditions: This symptom occurs when the hardware address is zero.
  Workaround: There is no workaround.

- **CSCtr06926**
  Symptoms: A CA server in auto grant mode goes into disabled state when it receives a client certificate enrolment request.
  Conditions: This symptom is observed when a client certificate enrolment request is received.
  Workaround: Do not place the CA server in auto grant mode.

- **CSCtr25386**
  Symptoms: BFDv6 static route association fails after reenabling interfaces.
  Conditions: This symptom is observed after interfaces are reenabled.
  Workaround: There is no workaround.

- **CSCtr31496**
  Symptoms: The line card crashes after switchover with the multilink configurations.
  Conditions: This symptom occurs after switchover with the multilink configurations.
  Workaround: There is no workaround.

- **CSCtr35740**
  Symptoms: QoS queuing hierarchy not moved to current active link when the previously active link goes down.
  Conditions: This symptom is observed when the DMVPN tunnel active link goes down.
  Workaround: There is no workaround.

- **CSCtr49064**
  The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability. Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh
• CSCtr51926
Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.
Conditions: This symptom is observed when a service-policy is applied on the main interface.
Workaround 1: Enable IPv6 explicitly on the main interface:

```bash
interface x/y
ipv6 enable
```

Workaround 2: Reconfigure the IPv6 address on the subinterface:

```bash
interface x/y.z
no ipv6 address
ipv6 address ...
```

• CSCtr56174
Symptoms: The MPLS-TE link count reaches a large value (4 billion+) on the Cisco ASR 1000 series router and negative value on the Cisco 7600 series router. This issue is seen in the `show mpls tr link sum` and `show mpls tr link int` command output.
Conditions: This symptom occurs if MPLS-TE tunnels are deleted using the `no int tunX` command and if the number of TE tunnels deleted are more than the TE links on the box. Even if they are not, with every TE tunnel deleted, the link count is affected and gets reduced.
Workaround: Do not delete MPLS-TE tunnels using the `no int tuX` command. If a TE tunnel is not required, shut it down. If these symptoms are observed, the only way is to reboot.

• CSCtr58140
Symptoms: PFR-controlled EIGRP route goes into Stuck-In-Active state and resets the neighbor.
Conditions: This symptom is observed when the PFR inject route in an EIGRP topology table after the policy decision. The issue was first seen on an MC/BR router running PFR EIGRP route control and with EIGRP neighbors over GRE tunnels.
Workaround: There is no workaround.

• CSCtr79347
Symptoms: The Cisco ASR1006 crashes without a BGP configuration change or BGP neighbor up/down event.
`UNIX-EXT-SIGNAL`: Segmentation fault(11), Process = BGP Task

Traceback summary

```bash
% 0x80e7b6 : __be_bgp_tx_walker_process
% 0x80e3bc : __be_bgp_tx_generate_updates_task
% 0x7f8891 : __be_bgp_task_scheduler
```

Conditions: There is no condition. But, this is a rarely observed issue.
Workaround: There is no workaround.

• CSCtr81559
Symptoms: The PPP session fails to come up occasionally on the LNS due to a matching magic number.
Conditions: This symptom is observed during LCP negotiation, when the random magic number generated on the client matches the magic number generated on the LNS. PPP assumes it to be a loopback and disconnects the PPP session. This condition occurs rarely.
Workaround: To avoid this, renegotiate the LCP. Configure the client using the `retry` command. This may cause the next session to come up correctly. CSCtr91106

A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS Software are not vulnerable.
Cisco has released free software updates that address these vulnerabilities.
The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.
This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

Symptoms: The RP crashes sometimes when the router is having PPPoX sessions.
Conditions: This symptom occurs if a PPPoX session is terminated in the middle of session establishment and “ip local pool” is configured to pick the IP address for the peer and the version that the router is running has the fix for CSCtr91890.
Workaround: There is no workaround.

Symptoms: The following log is seen, and VCs cannot be configured.
SSF CM: SSM switch id 0 [0x0] allocated
ACLIB [Gi9/1/0.3830, 3830]: Failed to setup switching for VLAN interface ...
Conditions: This symptom is observed with the access circuit interface shut and core flaps occurring, along with pseudowire redundancy. Also, leaks occur per flap.
Workaround: There is no workaround. If VCs can be removed, do so to release some IDs. Otherwise, try a redundancy switchover.

Symptoms: Longevity testing session churn causes RP crash on the Cisco ASR1000 router. RP crash occurs due to memory leak by the QOS Accounting feature.
Conditions: This symptom is observed during testing with the QOS Accounting feature PAC2. This issue is seen when there are a large number of sessions and churns with “aaa-accounting” in the QOS policy-map.
Workaround: There is no workaround.

Symptoms: PIM bidirectional traffic loops upon DF-election and RPF-change.
Conditions: This symptom is observed with several hundred streams combined with a routing change (interface shutdown/no shutdown or metric increment/decrement).

Workaround: There is no workaround.

- **CSCts34693**

  Symptoms: A Cisco router may crash with the following error message:

  ```
  000199: *Aug 23 16:49:32 GMT: %BGP-5-ADJCHANGE: neighbor x.x.x.x Up
  ```

  Exception to IOS Thread:
  Frame pointer 0x30CF1428, PC = 0x148FDF84

  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = EEM ED Syslog

  ```
  Exception trace:
  1#07279b80de945124c720ef5414c32a90 :10000000+48FDF84 :10000000+48FE400 :10000000+4B819C8 :10000000+4B81964 :10000000+F5FAD8 :10000000+F5FD10 :10000000+F5FF94 :10000000+F60608
  ```

  Conditions: This symptom is observed in a Cisco ASR 1004 router running Cisco IOS Release 15.0(1)S. This problem appears to be related to an EEM script that executes on a syslog event.

  ```
  event manager applet BGP-MON
  event tag BGP-DOWN syslog pattern "BGP-5-ADJCHANGE.*Down"
  event tag BGP-UP syslog pattern "BGP-5-ADJCHANGE.*Up"
  trigger
  correlate event BGP-DOWN or event BGP-UP
  action 02 cli command "enable"
  action 03 cli command "sh log"
  action 04 mail server "$_email_server" to "$_email_to" from "$_info_routername@mcen.usmc.mil" subject "Problems on $_info_routername, BGP neighbor Change" body "$_cli_result"
  ```

  Workaround: There is no workaround.

- **CSCts38429**

  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:


- **CSCts42154**

  Symptoms: After the Cisco IOS ASR 1006 router is reloaded, it fails to reregister to the key server. From the debugs, it is observed that the attempt to register is generated too early before the GDOI is ON. This registration attempt is made before the interface, through which GDOI registration traffic with the key server passes, goes to the UP state.

  Conditions: This symptom is observed on a Cisco IOS ASR 1006 router that runs Cisco IOS Release 15.0(1)S2 and Cisco IOS Release 15.0(1)S3.

  Workaround: Use the `clear crypto gdoi` command to fix this issue.

- **CSCts57115**

  Symptoms: After the following procedure is executed, multicast traffic on several VRFs is not forwarded to the outbound tunnel interface for MDT.

  The procedure is as follows:

  1. Reload the router.
2. Perform RP switchover.

3. Perform active ESP(F0) hardware reload.

4. Perform active ESP(F1) hardware reload.

Conditions: This symptom is observed when MVPN sends out multicast traffic on a lot of VRFs.

Workaround: Use the `ip pim sparse-mode` command to reconfigure the loopback0 (global) interface.

- CSCts62082
  
  Symptoms: Router generates the following message:

  %NHRP-3-QOS_POLICY_APPLY_FAILED: Failed to apply QoS policy 10M-shape mapped to NHRP group xx on interface Tunnelxx, to tunnel x.x.x.x due to policy installation failure

  Conditions: This symptom is observed when “per-tunnel” QoS is applied and there are more than nine DMVPN spokes. (Up to eight spokes, with QoS applied is fine.)

  Workaround: There is no workaround.

- CSCts64539
  
  Symptoms: The BGP next hop is inaccessible. The `show ip route` command output in the global and VRF routing tables shows that the next hop is reachable. The `show ip bgp vpnv4 all attr next-hop` command output shows max metric for the next hop.

  Conditions: This symptom occurs when an import map uses the “ip vrf name next-hop” feature while importing single-hop eBGP routes from the global routing table to the VRF routing table.

  Workaround 1: If “set ip next-hop” is not configured in import route map, this issue does not occur.

  Workaround 2: If “neighbor x.x.x.x ebgp-multihop” is configured, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

  Workaround 3: If “neighbor x.x.x.x disable-connected-check” is configured for a single-hop eBGP, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

- CSCts69204
  
  Symptoms: PPPoE sessions do not get recreated on the standby RP.

  Conditions: This symptom occurs on the standby RP.

  Workaround: There is no workaround.

- CSCts80643
  
  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  A workaround is available to mitigate this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:


- CSCts81427
  
  Symptoms: With a scaled dLFIoATM configuration on FlexWAN, after issuing SSO, some of the interfaces stop pinging.
Conditions: This symptom is observed after doing SSO.
Workaround: Shut/no shut of the ATM interface helps to resolve the problem.

• CSCts86788
Symptoms: CPU Hog messages start to appear, followed by a crash.
Conditions: This symptom is observed when the show mpls traffic-eng fast-reroute database interface name detail command is issued on an interface where there are no MPLS-TE tunnels.
Workaround: Do not issue this command on an interface where there are no MPLS-TE tunnels.
Further Problem Description: The trigger is simple, that is, issuing the FRR show display command on an interface on which there are no MPLS-TE tunnels.

• CSCts88467
Symptoms: The drops happen earlier than expected.
Conditions: This symptom occurs if the queue-limit is incorrectly calculated.
Workaround: Configure a queue-limit explicitly to fix this issue.

• CSCts90734
Symptoms: IKEA message trace entry memory leak is seen.
Conditions: This symptom occurs when there is an IPsec session.
Workaround: There is no workaround.

• CSCtt16487
Symptoms: High CPU is seen when changes are made to the Cisco WCCP Access Control List (ACL).
Conditions: This symptom is observed in a Cisco WCCP ACL.
Workaround: There is no workaround.

• CSCtt26643
Symptoms: A Cisco ASR 1006 router running Cisco IOS Release 15.1(2)S2 or Cisco IOS Release 15.1(3)S0a crashes with Signal 11.
Conditions: This symptom is observed on a Cisco ASR 1006 router running the asr1000rp1-adventerprisek9.03.04.00a.S.151-3.50a.bin image. The show version command causes the “Last reload reason: Critical software exception” error.
Workaround: There is no workaround.

• CSCtt32165
Symptoms: The Cisco Unified Border Element Enterprise on the Cisco ASR 1000 series router can fail a call with cause 47 immediately after the call connects.
Conditions: This symptom is observed with a sufficient call volume and a call flow that redirects many calls. The Cisco ASR router can fail to provision the forwarding plane for the new call due a race condition where a prior call is not completely cleaned up on the forwarding plane before trying to use the same structure again.
The show voice fpi stats command output indicates that a failure has occurred if the last column is greater than zero. For example:

```
show voip fpi stats | include provisn rsp
provisn rsp 0 32790 15
```
Workaround: There is no workaround. However, Cisco IOS Release 3.4.1 is less impacted by these call failures due to a resolution of defect CSCts20058. Upgrade to Cisco IOS Release 3.4.1 until such time as this defect is resolved. In a fully redundant Cisco ASR 1006 router, you can failover the ESP slots to clear the hung entries in the forwarding plane. Other platforms will require a reload.

- **CSCtt33158**
  
  **Symptoms:** If WRED is already present and the queue limit is configured in packets, then the WRED threshold become 0.

  **Conditions:** This symptom is observed if WRED is already present and the queue limit is configured in packets.

  **Workaround:** Remove WRED and reattach it.

- **CSCtt35936**
  
  **Symptoms:** EIGRP route updates are not sent to DMVPN spokes. The `show ip eigrp interface` command output shows pending routes in interface Q, which remains constant. The `show ip eigrp interface detail` command output shows that the next sequence number of the interface remains the same (does not advance).

  **Conditions:** This symptom occurs when EIGRP session flapped, resulting in routes being withdrawn and restored.

  **Workaround:** Add a static route on any spoke that kicks out EIGRP learned routes from the RIB table; this will again kick the interface on the HUB.

- **CSCtt69984**
  
  **Symptoms:** The Cisco ASR 1000 series router does not initialize GDOI registration for the second GDOI group after reload.

  **Conditions:** This symptom is observed with the following conditions:

  1. Image version: Cisco IOS Release 15.1(3)S
  2. Platform: Cisco ASR 1000 series router
  3. Two GDOI groups need to be configured.

  **Workaround 1:** Issue the `clear crypto gdoi` after the router reloads, or remove the crypto map from the WAN interface and reapply it.

  **Workaround 2:** If you are using the same local address for different GDOI groups, have the two groups use a different local address.

- **CSCtt90672**
  
  **Symptoms:** CFM MEP enters the INACTIVE state on deleting the subinterface.

  **Conditions:** This symptom is observed under the following conditions:

  1. Create a subinterface (vlan 104) for EOAM communication. Check “CC-Status” = Enabled.
  2. Create a QinQ subinterface (vlan tags: 104 128) for subscriber on the same physical interface. Check “CC-Status” = Enabled.
  3. Later, delete the QinQ subinterface from the step 2 above (DT’s provisioning system does it, for example, for a new policy change). The “CC-Status” goes to inactive.

  **Workaround:** Unconfigure and reconfigure the `continuity check` command under the corresponding Ethernet CFM domain/service global configuration for this CFM MEP.
• CSCtu01172
Symptoms: The Cisco ASR 1000 series router without an actual redundant router may crash when configured for CUBE HA based on the document “Cisco Unified Border Element High Availability(HA) on ASR platform Configuration Example”.
Conditions: This symptom is observed with the Cisco ASR 1000 series router.
Workaround: Remove the application configuration, that is, “no application redundancy”.

• CSCtu08608
Symptoms: The standby RP crashes due to Voip HA Session App.
Conditions: The Cisco ASR 1000 platform with redundant RPs and Cisco Unified Border Element Enterprise. The signature in the crashinfo is as follows:
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Voip HA Session App
Workaround: There is no workaround.

• CSCtu31340
Symptoms: The show sip call called-number crashes the router.
Conditions: This symptom is observed when the call SIP state is DISCONNECT.
Workaround: There is no workaround.

• CSCtu33956
Symptoms: The dialer with PPP encapsulation is seen when DSL is the WAN interface. L2PT does not work.
Conditions: This symptom is observed under the following conditions:
- The PPPoE dialer client needs to be configured on the physical SHDSL interface.
- The GRE tunnel destination interface should point to the dialer interface.
- The MPLS pseudowire should go over the tunnel interface.
- After the PPPoE session is set up, the GRE tunnel traffic gets dropped at the peer end of the PPPoE session.
Workaround: There is no workaround.

• CSCtw45168
Symptoms: DTMF interworking fails when MTP is used to convert OOB--RFC2833 and vice versa.
Conditions: This symptom occurs when MTP is used to convert OOB--RFC2833 and vice versa. This issue is seen starting from Cisco IOS XE Release 3.2S. Cisco IOS Release XE 3.1S should work fine.
Workaround: There is no workaround.

• CSCts76410
Symptoms: A tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.
Conditions: This symptom is observed during a rekey when the IPSec lifetime is high and the control packets do not reach the peer. This issue was observed with Cisco IOS Release 12.4(20)T and Cisco IOS Release 15.0(1)M7.
Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.
Caveats in Cisco IOS XE 3.4S Releases

OL-23288-23

CSCtt28703
Symptoms: The VPN client with RSA-SIG can access a profile where his CA trustpoint is not anchored.
Conditions: This symptom is observed when using RSA-SIG.
Workaround: Restrict access by using a certificate-map matching the right issuer.
PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.5/3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:P/I:N/A:N/E:POC/RLE:W/RC:C.
No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

CSCtu36562
Symptoms: cikeFailureReason and cipsecFailureReason from CISCO-IPSEC-FLOW-MONITOR MIB do not report the proper failure reasons for failed IKE negotiations (ph1 or ph2).
Conditions: This symptom is observed with failed IKE negotiations (ph1 or ph2).
Workaround: There is no workaround.

CSCtt94537
Symptoms: Auth_length of a BFD multihop packet is 0.
Conditions: This symptom is observed when you configure BFD multihop with SHA or MD5.
Workaround: There is no workaround.

CSCt26643
Symptoms: A Cisco ASR 1006 router running Cisco IOS Release 15.1(2)S2 or Cisco IOS Release 15.1(3)S0a crashes with Signal 11.
Conditions: This symptom is observed on a Cisco ASR 1006 router running the asr1000rp1-adventerprisek9.03.04.00a.S.151-3.50a.bin image. The show version command causes the “Last reload reason: Critical software exception” error.
Workaround: There is no workaround.

CSCtv19529
Symptoms: The router crashes on unconfiguring the last available DHCP pool. The crash is also seen on running the no service dhcp command.
Conditions: This symptom can occur only if the “DHCP Client” process is running on the router, along with the DHCP relay processes (DHCPD Receive, DHCPD Timer, DHCPD Database).
The client process can be started:
1. From an DHCP autoinstall attempt during router startup (with no nvram config).
2. If the ip address dhcp is run on one of the interfaces.
3. If the router was used for DHCP proxy client operations.
The relay processes are started when a DHCP pool is created by the ip dhcp pool pool command.
Workaround: Have a dummy DHCP pool created using the ip dhcp pool dummy_pool command, and never delete this pool. Other pools can be created and removed at will. The dummy_pool should not be removed. In addition, do not execute the no service dhcp command.
• CSCtq68778
  Symptoms: After an ISSU, the reload reason string is missing in the newly-active session.
  Conditions: This symptom is observed after an ISSU.
  Workaround: There is no workaround.

• CSCtt18020
  Symptoms: A router that is running Cisco IOS may reload unexpectedly.
  Conditions: This symptom may be seen with active SSH sessions to or from the router. Only SSH is affected.
  Workaround: Use Telnet.

• CSCtr05686
  Symptoms: An error occurs when a policy-map with byte based queue-limit is not attachable to target.
  The above configuration is not possible.
  Conditions:
  This issue occurs only when bytes based wred is configured before byte based queue-limit.
  Workaround: See the following:

Open Caveats—Cisco IOS XE Release 3.4.1S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.4.1S.

• CSCtr79347
  Symptoms: The Cisco ASR1006 crashes without a BGP configuration change or BGP neighbor up/down event.
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Task
  Traceback summary ---------------
  % 0x80e7b6 : __be_bgp_tx_walker_process
  % 0x80e3bc : __be_bgp_tx_generate_updates_task
  % 0x7f8891 : __be_bgp_task_scheduler
Conditions: This symptom is observed when you change the BFD-related BGP configuration. This issue is also seen when there is no trigger.
Workaround: There is no workaround.

- CSCt84641
Symptoms: The misclassification issue occurs when using deny statements in the ACL for a class-map. If the packets match the deny statements, they may be not classified properly.
Conditions: This symptom occurs when you configure deny statements in the ACL for a class-map.
Workaround: There is no workaround.

- CSCt16013
Symptoms: Longevity testing session churn causes RP crash on the Cisco ASR1K router. The RP crash occurs due to memory leak by the QOS Accounting feature.
Conditions: This symptom is observed during testing with the QOS Accounting feature PAC2. This issue is seen when there are a large number of sessions and churns with “aaa-accounting” in the QOS policy-map.
Workaround: There is no workaround.

- CSCt22958
Symptoms: A crash occurs on the Cisco ASR-ESP when the internal memory related to fragments is exhausted.
Conditions: This symptom occurs when the internal memory related to fragments is exhausted and a jumbo packet (larger than 16K after reassembly) is dropped by ESP.
Workaround: There is no workaround.

- CSCt64130
Symptoms: Tunnel MTU is incorrectly calculated when the tunnel is configured with a tunnel protection. It shows a much higher value than the actual value.
Conditions: This symptom is observed on the Cisco ASR router running Cisco IOS Release 15.1(3)S0a.
Workaround: MTU on the egress physical interface can be lowered. However, if the tunnel is configured with “mpls ip”, there is no workaround.

- CSCt72164
Symptoms: In a large-scale DMVPN environment using BGP as the routing protocol, a DMVPN hub router may crash in the Cisco IOS process under high-scale conditions.
Conditions: This symptom occurs when there is a routing reconvergence in the network.
Workaround: There is no workaround.

- CSCt82679
Symptoms: The RP crashes on a Cisco ASR router related to crypto.
Conditions: This symptom occurs when crypto is configured.
Workaround: There is no workaround.

- CSCtr98684
Symptoms: This is a rare condition triggered by the combination of using “ip ospf network point-to-multipoint” and the packet forwarding implementation on the Cisco ASR platform.
Conditions: This symptom occurs when there are OSPF adjacency issues when using the Cisco ASR router with the “ip ospf point-to-multipoint” configuration. These issues are triggered by the timing of the neighbor formation over a “shared” segment.
Workaround: Change the network type to broadcast.

Resolved Caveats—Cisco IOS XE Release 3.4.1S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.1S.

- CSCtd15853
  Symptoms: When removing the VRF configuration on the remote PE, the local PE receives a withdraw message from the remote PE to purge its MDT entry. However, the local PE does not delete the MDT entry.
  Conditions: This symptom is observed with the following conditions:
  - mVPN is configured on the PE router.
  - Both Pre-MDT SAFI and MDT-SAFI Cisco IOS software is running in a Multicast domain.
  Multicast VPN: Multicast Distribution Trees Subaddress Family Identifier:
  Workaround: There is no workaround.

- CSCtj56551
  Symptoms: The Cisco 7600 crashes in a very rare case.
  Conditions: This symptom is observed very rarely when route-churn/sessions come up.
  Workaround: There is no workaround.

- CSCtk18404
  Symptoms: Per-user route is not installed after IPCP renegotiation.
  Conditions: This symptom is observed with the following conditions:
  1. When the PPP session comes up, NAS installs static routes which are sent as attribute from RADIUS server.
  2. After a while, if CPE asks for IPCP renegotiation, IPCP is renegotiated, but the static routes are lost.
  Workaround: There is no workaround.

- CSCtl09030
  Symptoms: The Cisco ASR1k configured to function as ISG and DHCP relay/server crashes in the ARP input process or IP inband session initiator process in dhcpd_find_binding function.
  Conditions: This symptom is observed when the Cisco ASR1k is configured with DHCP relay or server and DHCP initiated IP sessions are configured. This issue is seen when the ISG inband IP session initiator is configured and an ARP request is received from a client whose DHCP IP session has timed out or cleared.
  Workaround: Disable ISG DHCP session initiator.
- **CSCtn65116**
  Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.
  Conditions: This symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Cisco IOS Release 12.2(33)SRB and later. Earlier versions are not affected.
  Workaround: Advertise and withdraw or withdraw and readvertise a more specific prefix, which will force the reevaluation of the prefix not being imported, for import again.

- **CSCtn67034**
  Symptoms: The username attribute is missing in the accounting stop record even though the user is authenticated.
  Conditions: This symptom is observed when accounting is enabled for an unauthenticated session, and the start record does not have the username (as expected). After authenticating the session, the first accounting packet that goes out does not have the username, that is:
  1. The first interim packet, if interim is enabled.
  2. The stop record, if interim is not enabled or if the stop record is sent before the interim period expires.
  Workaround: Enable the interim so that the stop record will have the username information.

- **CSCto16196**
  Symptoms: Performing `no wccp version2` on the WAAS device connected to the WAN link and then reconfiguring `wccp version 2` results in tracebacks on a Cisco ASR 1000 router configured with WCCP. Traffic loss is also observed.
  Conditions: This symptom is observed when WCCP is configured on a Cisco ASR 1000 router and the WCCP tunnels are up before `wccp version 2` is removed and reapplied on the WAAS devices.
  Workaround: There is no workaround.

- **CSCto99343**
  Symptoms: Line cards do not forward packets, which causes a failure on the neighborship.
  Conditions: This symptom is observed on VSL-enabled line cards on a VSS system.
  Workaround: There is no workaround.

- **CSCtq17082**
  Symptoms: The router reloads.
  Conditions: This symptom is observed with at least 2000 IPSec tunnel sessions by automatic script to remove a QoS configuration from Virtual Template.
  Workaround: Session teardown before you remove the QoS configuration.

- **CSCtq21234**
  Symptoms: Label is not freed.
  Conditions: This symptom is observed after shutting down the link.
  Workaround: There is no workaround.

- **CSCtq24614**
  Symptoms: The commands to ignore S1 bytes are not supported on an ATM interface.
  Conditions: This symptom is observed with an ATM SPA.
  Workaround: There is no workaround.
- CSCq58383
  Symptoms: A crash occurs when modifying or unconfiguring a loopback interface.
  Conditions: This symptom occurs while attempting to delete the loopback interface, after unconfiguring the “address-family ipv4 mdt” section in BGP.
  Workaround: Unconfiguring BGP may prevent the issue from happening without reloading the router.

- CSCq79350
  Symptoms: After changing the ACL in a key server a couple of times, the rekey will fail in the GM.
  Conditions: This symptom is observed when you add/remove an ACL in a key server.
  Workaround: Use the `clear crypto GDOI` command.

- CSCq80648
  Symptoms: If a user changes the VRF assignment, such as moving to another VRF, removing the VRF assignment, etc., on which a BGP IPv6 link-local peering (neighbor) is based, the BGP IPv6 link-local peering will no longer be able to delete or modify.
  Conditions: This symptom occurs when a user changes the VRF assignment.
  Workaround: Remove the BGP IPv6 link-local peering before changing the VRF assignment on the interface.

- CSCq86515
  Symptoms: UDP Jitter does not detect packet loss on Cisco IOS Release 15.1.
  Conditions: This symptom occurs when traffic is dropped on the device sending the UDP Jitter probe. However, when traffic is dropped on another device, packet loss is detected.
  Workaround: Do not drop traffic on the device sending the UDP Jitter probe.

- CSCq91643
  Symptoms: The basic IP session with dot1q encapsulation and IP initiator may not come up.
  Conditions: This symptom is observed on an ES40.
  Workaround: Reconfigure the dot1q encapsulation (which has the same VLAN ID as the outer VLAN ID of the QinQ subinterface) after an OIR.
• CSCtq96329
Symptoms: The router fails to send withdraws for prefixes, when “bgp deterministic-med” is configured. This could lead to traffic blackholing and routing loops and could also result in memory corruption/crash in rare conditions.
Conditions: This symptom can occur only when “bgp deterministic-med” is configured. The following releases are impacted:
- Cisco IOS Release 15.0(1)S4
- Cisco IOS Release 15.1(2)T4
- Cisco IOS Release 15.1(3)S
- Cisco IOS Release 15.2(1)T

Workaround: Disable deterministic med in the network/AS by issuing the no bgp deterministic-med command and then the clear ip bgp * command or by performing hardreset of the BGP session to remove any stale prefixes.
It is further recommended to do an SSO on routers that are running the impacted software to eliminate any potential corruption that might have already existed on routers that are running the impacted software.
Further Problem Description: If deterministic med is enabled, withdraws are not sent.

• CSCtr05003
Symptoms: The Cisco ASR1000 with SIP calls crashes from RTPSPI.
Conditions: This symptom is observed with H323 and SIP configurations on the router.
Workaround: There is no workaround.

• CSCtr07704
Symptoms: While using scripts to delete a nonexistent class map filter from a class, the router sometimes crashes (c2600XM) or returns traceback spurious memory access (c2801nm).
Conditions: This symptom occurs when trying to delete a nonexistent classmap filter. The classmap will be NULL and passed to match_class_params_same; this results in referencing a null pointer.
Workaround: Do null check in match_class_command and match_class_params_same. To keep the existing behavior, do not print out a message like “the class does not exist” when deleting a nonexistent class map from a class.

• CSCtr14675
Symptoms: The line card crashes after removing the child policy in traffic.
Conditions: This symptom occurs after the child policy is removed in traffic.
Workaround: There is no workaround.

• CSCtr18708
Symptoms: SMI can be configured on Gigabit Ethernet0 on the Cisco ASR1k router.
Conditions: This symptom occurs on the Cisco ASR1k router.
Workaround: Do not configure SMI on Gigabit Ethernet0 because it is unsupported (see CSCta28011 and the SMI configuration guide).

• CSCtr19922
Symptoms: Lots of output is printed by the show adjacency [key of adj] internal dependents command, followed by a crash.
Conditions: This symptom is observed with the existence of midchain adjacencies, which will be created by IP tunnels, MPLS TE tunnels, LISP, and similar tunneling technologies.

Workaround: Do not use the `show adjacency [key of adj] internal dependents` command. Specifically, it is the `dependents` keyword that is the problem. If the `dependents` keyword is not used, there is no problem.

- **CSCtr22007**
  Symptoms: A Cisco 7600 router that is configured with RSVP crashes.
  Conditions: This symptom is observed with MPLS-TE tunnel flap.
  Workaround: There is no workaround.

- **CSCtr28857**
  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link: [http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp](http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp)

- **CSCtr30621**
  Symptoms: When working and protect LSPs are over different IMs, an OIR of one will bring down both.
  Conditions: This symptom is observed when you OIR the link for one LSP.
  Workaround: Shut/no shut the TP tunnel interface.

- **CSCtr45608**
  Symptoms: Referring an IPv6-only VRF on a route-map crashes the router.
  Conditions: This symptom is observed on a Cisco Catalyst 4000 Series Switch when “set vrf” is configured on the route-map and the VRF is IPv6 only.
  Workaround: Configure “ipv4 vrf”, along with “ipv6 vrf” and refer “ipv6 vrf” on the route-map by configuring “ipv6 policy” on the ingress interface.

- **CSCtr45633**
  Symptoms: A BGP dynamic neighbor configured under VPNv4 address-family does not work correctly.
  Conditions: This symptom is observed when a BGP dynamic neighbor is configured under a VPNv4 address-family.
  Workaround: Add “dynamic neighbor peer-group” under “ipv4 unicast address-family”.

- **CSCtr51786**
  Symptoms: The `passive-interface` command for a VNET auto-created subinterface x/y.z may remove the derived interface configuration command `ip ospf process id area number`. Consequently, putting back the `no passive-interface` command will not form the lost OSPF ADJ.
  Conditions: This symptom is observed only with interfaces associated with the OSPF process using the `ip ospf vnet area number` command.
  Workaround: Associate the interface with the OSPF process using a network statement or using the interface command `ip ospf process id area number`. 
Further Problem Description: Interfaces associated with a process using a network statement under “router ospf” or interfaces configured with the `ip ospf` process id area number command are not affected.

- CSCtr57226

Symptoms: The Cisco ASR router with CUBE Enterprise and the Cisco IOS SW MTPs configured can result in an MTP leak, leading to the Cisco ASR router rejecting calls with cause 47.

Conditions: This symptom is observed when the SCCP Application process increases in memory size due to a leak. Eventually, the leaking SCCP process results in calls rejected with cause 47. The ASR CUBE must have software MTPs configured, as given below:

```
dspfarm profile x
mtp maximum sessions software y
associate application sccp
```

The following `show` command indicates whether the SCCP Application is leaking sessions:

```
sh mem debug leak chunk
```

Adding blocks for GD...

<table>
<thead>
<tr>
<th>Address</th>
<th>Size</th>
<th>Alloc_pc</th>
<th>PID</th>
<th>Alloc-Proc</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor memory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30796D18</td>
<td>300</td>
<td>D927C74</td>
<td>64</td>
<td>IOSD ipc task</td>
<td>IOSD ipc task</td>
</tr>
<tr>
<td>479D651C</td>
<td>57140</td>
<td>124C946C</td>
<td>438</td>
<td>SCCP Application</td>
<td>RTPSPI_DEQUEUE_EVENT</td>
</tr>
<tr>
<td>489C6700</td>
<td>57140</td>
<td>124C946C</td>
<td>438</td>
<td>SCCP Application</td>
<td>RTPSPI_DEQUEUE_EVENT</td>
</tr>
<tr>
<td>48B153ED</td>
<td>57140</td>
<td>124C946C</td>
<td>438</td>
<td>SCCP Application</td>
<td>RTPSPI_DEQUEUE_EVENT</td>
</tr>
<tr>
<td>48B667EC</td>
<td>57140</td>
<td>124C946C</td>
<td>438</td>
<td>SCCP Application</td>
<td>RTPSPI_DEQUEUE_EVENT</td>
</tr>
<tr>
<td>499468FC</td>
<td>57140</td>
<td>124C946C</td>
<td>438</td>
<td>SCCP Application</td>
<td>RTPSPI_DEQUEUE_EVENT</td>
</tr>
<tr>
<td>4A5661EC</td>
<td>57140</td>
<td>124C946C</td>
<td>438</td>
<td>SCCP Application</td>
<td>RTPSPI_DEQUEUE_EVENT</td>
</tr>
</tbody>
</table>

Workaround: To resolve the issue, try issuing the following commands:

```
conf t
no sccp
pause until SCCP cleanup is complete
sccp
end
```

If this method is not successful, the Cisco ASR router will need to be reloaded to recover the memory from the leaked MTP sessions.

- CSCtr66878

Symptoms: Login to Cisco ASR 1002 routers fails.

The logs are as follows:

```
%CPPOSLIB-3-ERROR_NOTIFY: F0: fman_fp_image: fman-fp encountered an error
 Traceback= 1#78702a22f7c824a946f5e71990873d4b errmsg=D39B000+2160
 cpp_common_os:B93C000+B620 cpp_common_os:B93C000+189B8 cpp_sbs:B828000+AA98
 cpp_sbs:B828000+79E4 cpp_sbs:B828000+7E1C cpp_sbs:B828000+7FC4
 cpp_cef_mpls_common:BC96000+43728 cpp_cef_mpls_common:BC96000+441FC
 :10000000+1C2B94 evlib:C5CF000+DABC evlib:C5CF000+FFC4 :10000000+14EF00
 c:A381000+1E938 c:A381000+1EAE0
%IOSXE-6-PLATFORM: F0: cpp-cdm: Shutting down CPP MDM while client(s) still connected
%CPPHA-3-CDMDONE: F0: cpp_ha: CPP 0 microcode crashdump creation completed.
%IOSXE-6-PLATFORM: F0: cpp_ha: Shutting down CPP MDM while client(s) still connected
%IOSXE-6-PLATFORM: F0: cpp_ha: Shutting down CPP CDM while client(s) still connected
```
%PMAN-3-PROCHOLDDOWN: F0: pman.sh: The process cpp_cdm_svr has been helddown (rc 69)
%PMAN-3-PROCHOLDDOWN: F0: pman.sh: The process cpp_ha_top_level_server has been helddown (rc 69)
%FMFP_QOS-6-QOS_STATS_STALLED: F0: fman_fp_image: statistics stalled
%ASR1000_OIR-6-ONLINECARD: Card (fp) online in slot F0
%IOSXE-6-PLATFORM: F0: cpp_cp: Process CPP_PFILTER_EA_EVENT__API_CALL__REGISTER

The router recovers by itself.

Conditions: This symptom is observed when the Cisco ASR 1002 router is running Cisco IOS Release 12.0(1)S3 and has a zone-based firewall configured.

Workaround: Do not delete class-default from the policy map.

- CSCtr89882
  Symptoms: Platform-related error messages are seen during an LDP flap in an ECM scenario.
  Conditions: This symptom is observed with LDP with ECMP paths and during flapping of LDP sessions.
  Workaround: There is no workaround.

- CSCti83542
  Symptoms: MPLS LDP flapping is seen with T3 SATOP CEM interface configurations.
  Conditions: This symptom is observed with T3/E3 SATOP TDM configurations.
  Workaround: There is no workaround.

- CSCto76700
  Symptoms: The multihop BFD session goes down with TE-FRR cutover.
  Conditions: This symptom may be observed with single hop, VCCV BFD, and multihop BFD sessions. However, after the TE-FRR cutover, the VCCV BF session comes back up, whereas the multihop BFD session goes down.
  Workaround: The workaround is to perform a “no shut” on the port-channel interface.

- CSCtr80366
  Symptoms: Relay miscalculates the giaddr from the OFFER packet, and hence cannot find the binding.
  Conditions: This symptom occurs while configuring multiple pools on the server and multiple secondary IP addresses on the relay loopback IP address.
  Workaround: There is no workaround.

- CSCts39240
  Symptoms: The advertise command is not available in BGP peer-policy templates.
  Conditions: This symptom is observed on Cisco router running Cisco IOS Release 15.2(01.05)T, Cisco IOS Release 15.2(00.16)S, Cisco IOS Release 15.1 (03)S0.3, or later releases.
  Workaround: The keyword and functionality is still available to be configured in the BGP neighbor command.

- CSCts39535
  Symptoms: BGP IPv6 routes that originate from the local router (via network statements or redistribute commands) fail to match any specified condition in an outbound route map used on a neighbor statement, regardless of the expected matching results. Thus, the route map may not be applied correctly, resulting in erroneous filtering or advertising of unintended routes.
Further testing revealed that the “suppress-map” and “unsuppress-map” commands (used in conjunction with the “aggregate-address” command) are also broken, in the sense that the route-map filtering will fail to correctly suppress or unsuppress a subnet under the aggregated prefix.

Conditions: This symptom is observed when an outbound route map with a match statement is used in a “neighbor” statement for an IPv6 or VPNv6 neighbor in BGP, and there are locally originated routes, either through network statements or by redistribution. All “match” statements, except for “as-path”, “community”, and “extcommunity” are impacted; this includes match ipv6 address, protocol, next-hop, route-source, route-type, mpls, tag.

Workaround: There is no workaround for the same router. However, inbound route maps work fine, so configuring inbound route maps on the neighboring router can compensate.

Another way to handle the issue would be to configure prefix lists directly on the network statement. So, filtering will be preserved. But, there will not be a way to “set” anything as route maps can typically do.

- CSCts45619

  Symptoms: T.38 Fax calls through the CUBE enterprise on the Cisco ASR platform with the Cisco IOS MTP colocated on the ASR can fail with cause 47 and subsequently leak a structure on the forwarding plane, causing future call failures.

  Conditions: This symptom is observed with T.38 calls through the CUBE enterprise on the Cisco ASR platform (only) with colocated MTPs in the call flow.

  Workaround: On nonredundant ASR platforms, a reload is required to clear the hung structures on the forwarding plane. On the Cisco ASR1006 with redundant RPs and ESPs, you can perform a switchover of the ESPs (FPs) to clear the problem, as follows:

  ```
  hw-module slot F0 reload
  ! confirm via show platform that the F0 is in a ok, standby state, takes some time for the F0 to reload.
  sh platform
  ! do not execute the below command until F0 is back online
  hw-module slot F1 reload
  ! again, confirm via show platform that the F1 is in a ok, standby state
  sh platform
  ```

- CSCts46507

  Symptoms: Runtime Priority does not get back to the original value set as priority.

  Conditions: This symptom is observed when the tracked interface is flapped.

  Workaround: There is no workaround.

- CSCts47605

  Symptoms: For ECMP on the Cisco ASR1k router, RSVP does not select the right outgoing interface.

  Conditions: This symptom is observed with RSVP configuration with ECMP.

  Workaround: There is no workaround.

- CSCts51980

  Symptoms: STM1-SMI PAs of version 3.0 do not come up.

  Conditions: This symptom is observed when the new version of PAs do not come up with enhanced flexwan.

  Workaround: There is no workaround. Without the PA, flexwan will come up.
- CSCts67423

Symptoms: On the Cisco ASR1k and ISR G2 only, call failures occur in the CUBE enterprise with interoperability to third-party SIP devices due to a trailing comma in the Server and User-Agent fields. For example:


You might see this with Cisco IOS Release 15.2(1)T or other versions. If the trailing comma is present it can cause interoperability issues. If there is no trailing comma, then this defect is not applicable.

Conditions: This symptom is observed when there is an interoperability problem between the CUBE enterprise and a third-party SIP device. The trailing comma is invalid against RFC 2616 and the third-party SIP device ignores SIP messages from the CUBE.

Workaround: On both inbound and outbound dial peers, apply a SIP profile similar to the one below, or add the four lines to an existing SIP profile in use.

```
voice class sip-profile 1
    request ANY sip-header User-Agent modify "-15.*", ""
    response ANY sip-header User-Agent modify "-15.*", ""
    request ANY sip-header Server modify "-15.*", ""
    response ANY sip-header Server modify "-15.*", ""
dial-peer voice 1 voip
    voice-class sip profiles 1
```

- CSCts76964

Symptoms: The Cisco ASR router crashes with tracebacks, as given below:

Exception to IOS Thread:
Frame pointer 0x7F5CED910380, PC = 0x2F4A2E7

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Crypto IKMP
-Traceback=
1#261f9625131701783f9129d7afdd6633 :4000000+2B4A2E7 :4000000+4FAFFBF :400000+4FBC6F2
BC2FB :400000+4FBC6F2
:400000+371635B :400000+63E08B6 :400000+63DC863 :400000+63F13A6 :400000+63F15
6D :400000+629144E :4
00000+63E51A1 :400000+64BE0B1 :400000+64BE037 :400000+63ED59 :400000+624BBB6
:400000+63BC34

Fastpath Thread backtrace:
-Traceback= 1#261f9625131701783f9129d7afdd6633 c:7F5DE3D0F000+BDDD2

Auxiliary Thread backtrace:
-Traceback= 1#261f9625131701783f9129d7afdd6633 pthread:7F5DE1D0E000+A7C9

RAX = 0000000000000000 RBX = 006DE6F05C7F0000
RCX = 0000000000000000 RDX = 0000000000000000
RSP = 00007F5CED910380 RBP = 00007F5CED9103A0
RSI = 0000000000000000 RDI = 406D0D0A00000000
RB = 00000000F0466060 R9 = A038E6F05C7F0000
R10 = 00000000A0F96B8 R11 = 8038E6F05C7F0000
R12 = 0000000000000000 R13 = 00007F5CF0A51A80
R14 = 406D0D0A00000000 R15 = 0000000000000000
RFL = 000000000010246 R1P = 000000002F4A2E7
CS = 0033 FS = 0000 GS = 0000
ST0 = 0000 0000000000000000 ST1 = 0000 0000000000000000
ST2 = 0000 0000000000000000 ST3 = 0000 0000000000000000
ST4 = 0000 0000000000000000 ST5 = 0000 0000000000000000
ST6 = 0000 0000000000000000 ST7 = 0000 0000000000000000
X87CW = 037F X87SW = 0000 X87TG = 0000 X87OP = 0000
Caveats in Cisco IOS XE 3.4S Releases

Conditions: This symptom is observed under the following conditions:

- GETVPN is operational on the Cisco ASR router.
- Registration to the Key-Server happens over the physical links.
- There is one primary and secondary link to the Key-Server.
- The crypto map is enabled on the primary interface first. Everything works fine here.
- The crypto map is enabled on the secondary interface. The ASR crashes as soon as you enable it on the Secondary interface with tracebacks, as shown above.
- The crash is also observed if the secondary interface is down and the crypto map is applied on it, although the crash is not observed instantly.
- The issue is also observed in Cisco IOS Release 15.1(3)Sa, along with Cisco IOS Release 12.2(33)XNE (could be reproduced only once at the first instance, and was not seen in subsequent tries) and Cisco IOS Release 12.2(33)XNF2.

When the same GDOI crypto-map is applied to two interfaces (in primary and secondary role), without the local-address configuration and TBAR enabled, and when KS sends the TBAR pseudotime update, the GM code gets confused between the two interfaces and the crash is observed. It is considered to be more of a timing issue.

Workaround 1: Disable TBAR on the Key-Server, that is, either with no replay or by changing it to counter-based to resolve the issue.

Workaround 2: Use the `crypto map name local-address logical-address` command globally on the Cisco ASR router and let the registration happen through the loopback. The loopback should be reachable to the Key-Server over the primary and the secondary links, respectively. Then, enable the crypto map on the primary and secondary interfaces, which will work fine.

- CSCto58710

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

Conditions: This symptom is observed when a Cisco ASR 1000 series router attempts to retrieve a CRL using LDAP, and the LDAP server is in a VRF.

Workaround: Use a certificate map to revoke certificates or publish the CRL to an HTTP server and configure “CDP override” to fetch the CRL.
Resolved Caveats—Cisco IOS XE Release 3.4.0aS

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.0aS.

- CSCtq96329
  Symptoms: Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.
  Conditions: This symptom can happen only when bgp deterministic-med is configured.
  The following releases are impacted:
  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T
  Workaround: Disable deterministic med in the network/AS by issuing the `no bgp deterministic-med` command and then the `clear ip bgp*` command or hardreset of BGP session to remove any stale prefixes.

Resolved Caveats—Cisco IOS XE Release 3.4.0S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.0S.

- CSCto03123
  Symptoms:
  1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
  2. Additional memory leak can occur when frequent sensor value changes take place.
  Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.
  Workaround: There is no workaround.
  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.
  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.
  Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

Open Caveats—Cisco IOS XE Release 3.4.0S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.4.0S.

- CSCto16377
  Symptoms: DPD deletes only IPSec SAs. It does not delete IKE SAs.
Conditions: This issue is observed when DPD is enabled and the peer is down.
Workaround: There is no workaround.

- **CSCto45782**
  Symptoms: When a tunnel interface in a DMVPN environment flaps, about 10 percent of the original number of tunnels do not get re-established automatically.
  Conditions: This issue is observed when all the following conditions are met:
  - RP2 and ESP20 are installed on the router.
  - The DMVPN hub has a large number, for example, 4000, of spokes connected to traffic.
  - IKEv1 and EIGRP are configured on the DMVPN hub.
  Workaround: Re-establish the tunnels by manually clearing them using the `clear crypto sa peer` command or the `clear crypto isakmp` command.

- **CSCto56161**
  Symptoms: Memory leaks are observed when approximately one-fourth of the total number of ISGv6 PPP sessions start flapping.
  Conditions: This issue is observed when ISGv6 PPP sessions start flapping.
  Workaround: Reload the router.

- **CSCto91593**
  Symptoms: Packet loss is observed after an RPSO.
  Conditions: This issue is observed after an RPSO.
  Workaround: Run the `ip multicast redundancy routeflush` command. For example:
  ```
ip multicast redundancy routeflush maxtime 300
  ```

- **CSCto93005**
  Symptoms: A fatal error is observed on the ATM SPA when the `redundancy force-switchover` command is run on the peer router.
  Conditions: This issue is observed when both the following conditions are met:
  - AToM circuits are configured with a scale level of 1000 on the SPA.
  - Both like-to-like VCs and like-to-unlike VCs are configured on the SPA.
  Workaround: There is no workaround.

- **CSCto93031**
  Symptoms: Bulk synchronization failure is observed when the `scgp config` command is run.
  Conditions: This issue is observed when the `scgp config` command is run.
  Workaround: There is no workaround.

- **CSCto98249**
  Symptoms: The router crashes while re-enabling OSPFv3 on an interface.
  Conditions: This issue is observed when a large number of routes, for example, 1200000, are added.
  Workaround: There is no workaround.

- **CSCtq14556**
  Symptoms: If the active channel flaps while the standby channel is down, the multilinks do not come up.
Conditions: This issue is observed if the active channel flaps while the standby channel is down. The MLP bundles remain inactive because the interfaces are down due to an LRDI error.

Workaround: Bring up the standby channel.

- CSCtq15058
  Symptoms: A policy does not get attached to the LC after the policy map is modified and an OIR is performed.
  Conditions: This issue is observed after the policy map is modified and an OIR is performed.
  Workaround: There is no workaround.

- CSCtq17082
  Symptoms: The VTEMPLATE Background Mgr process crashes when QoS configurations are removed from the virtual template.
  Conditions: This issue is observed when there are at least 2000 IPSec tunnel sessions and an automated script is used to remove the QoS configurations from the virtual template.
  Workaround: There is no workaround.

- CSCtq17666
  Symptoms: Packets are dropped when the IP address is changed in the MSR.
  Conditions: This issue is observed when the IP address is changed in the MSR.
  Workaround: Reset the Vif1 interface.

- CSCtq24245
  Symptoms: If there are a large number of calls per session, new sessions do not come up due to resource shortage.
  Conditions: This issue is observed when there are a large number of calls per session.
  Workaround: There is no workaround.

- CSCtq28663
  Symptoms: The memory usage of Cisco ASR1000-SIP10 is very high and reaches the threshold value.
  Conditions: This issue is observed with four SPAs configured and the committed memory set at 91 percent.
  Workaround: There is no workaround. Note that this issue does not affect functionality.

- CSCtq31954
  Symptoms: High CPU utilization is observed during the AAA per-user process.
  Conditions: This issue is observed when there are a large number, for example, 15000, of TAL sessions.
  Workaround: There is no workaround.

- CSCtq40115
  Symptoms: The offset list does not increment the metric by the correct value.
  Conditions: This issue is observed in the EIGRP classic mode.
  Workaround: Use the EIGRP named mode.

- CSCtq46189
  Symptoms: The ESP reloads automatically.
Conditions: This issue is observed when multiple OIR operations are performed on either an individual ATM-based SPA or the SIP in which an ATM SPA is installed. Under test conditions, this issue was observed after approximately 60 OIR operations.

Workaround: Manually reload the ESP at some stage before the number of consecutive OIR operations reaches 60.

- CSCtq57630
  Symptoms: Packets are lost due to high CPU utilization that occurs when a large number of data MDTs are configured at the same time.
  Conditions: This issue is observed when a large number of data MDTs are configured at the same time.
  Workaround: Configure a small number of data MDTs at a time.

- CSCtq67680
  Symptoms: When the SPA reloads, the event triggers a silent reload of the LC.
  Conditions: This issue is observed when a QoS policy is applied on the multilink bundle of the serial SPA.
  Workaround: There is no workaround.

- CSCtq67717
  Symptoms: The standby SUP gets reset continuously after an SSO is performed or after the standby SUP is manually reset.
  Conditions: This issue is observed when the archive command is applied.
  Workaround: There is no workaround.

- CSCtq71477
  Symptoms: When the redistribute connected metric 20000000 2 255 255 1500 command is run, the bandwidth is set to 4294967295 Kb.
  Conditions: There are no specific conditions under which this issue is observed
  Workaround: There is no workaround.

- CSCtq74691
  Symptoms: A buffer leak is observed at radius_getbuffer.
  Conditions: This issue is observed when a DHCP request is initiated from the client, following which a DHCP address is allocated from the server and a session comes up in the authenticating state. The buffer leak occurs at radius_getbuffer and may increase with each new session.
  Workaround: There is no workaround.

- CSCtq79350
  Symptoms: Rekey fails in the GM after the ACL is changed in the key server a few times.
  Conditions: This issue is observed after the ACL is added to or removed from the key server.
  Workaround: Use the clear crypto gdoi command.

- CSCtq80074
  Symptoms: The router crashes when the no ip trigger-authentication timeout 90 port 1 command is run.
  Conditions: This symptom is observed when the following sequence of commands is run:
  1. ip trigger-authentication timeout 90 port 1
2. **ethernet mac-tunnel virtual 4094**

3. **no ip trigger-authentication timeout 90 port 1**

Workaround: There is no workaround.

- **CSCtq80351**

  Symptoms: The SP crashes during a switchover in the RPR mode.

  Conditions: This issue is observed during a switchover in the RPR mode. The following failure and traceback messages are displayed when multicast scale configurations are performed:

  ```
  %SYS-SP-2-MALLOCFAIL: Memory allocation of 1708 bytes failed from 0x82148C4, alignment 32   Pool: I/O   Free: 2064   Cause: Memory fragmentation   Alternate Pool: None   Free: 0   Cause: No Alternate pool   -Process= "Pool Manager", ipt= 0, pid= 8   -Traceback= 81BA4D8z 8345490z 834ACB0z 82148C8z 835FC38z 835FF9Cz 83A301Cz 839D288z   CMD: 'sh redundancy state | inc peer state' 18:21:22 IST Tue Jun 7 2011   18:21:22.575 IST: %SYS-SP-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (27/2),process = SP Error Detection Process.   -Traceback= 0x8367AACz 0x821E7BCz 0x821EA94z 0x8E01830z 0x8BDDD60z 0x8E01A08z 0x96ED980z 0x96EBB34z 0x83A301Cz 0x839D288z
  ```

  Workaround: There is no workaround.

- **CSCtq88437**

  Symptoms: An IKEv2 memory leak results in an RP reload.

  Conditions: This issue is observed when approximately 4000 crypto maps are configured. The memory leak speed depends on the session scale numbers. Session flapping increases the memory leak.

  Workaround: There is no workaround.

- **CSCtq93505**

  Symptoms: The SIP-200 LC crashes.

  Conditions: This issue is observed when members are swapped across bundles during VLAN allocation.

  Workaround: There is no workaround.

- **CSCtq95291**

  Symptoms: The router crashes.

  Conditions: This issue is observed when the saved configuration is copied to the startup configuration.

  Workaround: There is no workaround.

- **CSCtq95873**

  Symptoms: Some IPSec tunnels (DMVPN spokes) fail after the first IKE rekey.

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

  - RP2 and ESP20 are installed on the router.
  - The DMVPN hub has a large number, for example, 4000, of spokes connected to traffic.
  - IKEv1 and EIGRP are configured on the DMVPN hub.

  Workaround: Reduce the number of tunnels (spokes) to 2000 or less.

- **CSCtq96244**
Symptoms: Traceback is observed on the Cisco ASR 1004 Router when an incoming IPSec packet contains invalid SPI.

Conditions: This issue is observed when the following steps are performed:
1. The class map and policy map are configured.
2. The class map and policy map are applied to the virtual loopback tunnel router interface.
3. Traffic is started.
4. The tunnel target is changed on both the tunnel head and the tail end by shutting down the interface with the preferred route. The QoS target interface moves to the next preferred route.
5. The tunnel is changed to a new target.

Workaround: There is no workaround.

- CSCtq96329
  Symptoms: Router fails to send withdraws for prefixes, when “bgp deterministic-med” is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.
  Conditions: This symptom can happen only when “bgp deterministic-med” is configured.
  The following releases are impacted:
  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

Workaround: Disable deterministic med in the network/AS by issuing the `no bgp deterministic-med` command and then the `clear ip bgp *` command or hardreset of BGP session to remove any stale prefixes.

It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtr01431
  Symptoms: An error is encountered during configuration synchronization.
  Conditions: This issue is observed when the following sequence of steps is performed:
  1. A loopback interface is created
  2. The macro interface range is configured for the loopback interface.
  3. The loopback interface is deleted.
  4. SSO is performed.

Workaround: There is no workaround.

- CSCtr10853
  Symptoms: The router crashes after running for about 10 days.
  Conditions: This issue is observed when all the following conditions are met:
  - There are 1000 or more mGRE tunnels with tunnel protection and using IKEv2.
  - Each mGRE tunnel is a BGP update source interface.
Workaround: There is no workaround.

- **CSCtr12618**
  
  Symptoms: If the ACL of a crypto map is modified, IPSec traffic stops getting forwarded until the tunnels are rekeyed.
  
  Conditions: This issue is observed when a crypto map is configured.
  
  Workaround: Run the `clear crypto session` command.

- **CSCtr14867**
  
  Symptoms: Static VTI tunnels terminating on a Cisco ASR 1000 series router that is using NAT-T due to a NAT rule in between the endpoints will fail to decapsulate traffic. The tunnel will build phase 1 and phase 2, the remote peer will show IPSec encapss and decaps, but the Cisco ASR 1000 series router will only show encapss with no decaps. This causes one-way outgoing traffic from the Cisco ASR 1000 series router side of the tunnel.

  ```
  ASR1000#sh cry ipsec sa
  interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 192.168.12.1
  protected vrf: (none)
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 192.168.15.1 port 4500
  PERMIT, flags=(origin_is_acl,)
  #pkts encaps: 1008, #pkts encrypt: 1008, #pkts digest: 1008
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  The Drop reason from the ASR is IpsecInput.
  ```

  Conditions: This symptom is observed on a Cisco ASR 1000 series router that is running Cisco IOS Release XE 3.3.1S with NAT-T tunnels using udp/4500 for encrypted traffic and static VTIs are in use.

  Workaround: Remove NAT and use ESP for encapsulating encrypted packets. Downgrade to Cisco IOS Release 15.1(2)S. Use dynamic VTIs.

- **CSCts95579**
  
  Symptoms: The “%CRYPTO-4-RECVD_PKT_INV_SPI” error is displayed with an unexpected/incorrect tunnel interface listed in the error message text.

  Conditions: This symptom occurs when shared tunnel protection is used. This issue is seen in a DMVPN environment.

  Workaround: There is no workaround. This is a cosmetic issue.

- **CSCto58710**
  
  Symptoms: Certificate validation fails when the CRL is not retrieved.
Conditions: This symptom is observed when a Cisco ASR 1000 series router attempts to retrieve a CRL using LDAP, and the LDAP server is in a VRF.

Workaround: Use a certificate map to revoke certificates or publish the CRL to an HTTP server and configure “CDP override” to fetch the CRL.
Caveats in Cisco IOS XE 3.3S Releases

This chapter provides information about caveats in Cisco IOS XE 3.3S releases.

Because Cisco IOS XE 3S is based on Cisco IOS XE 2 inherited releases, some caveats that apply to Cisco IOS XE 2 releases also apply to Cisco IOS XE 3S. For a list of the software caveats that apply to Cisco IOS XE 2, see the “Caveats for Cisco IOS XE Release 2” section at the following location:


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


This chapter contains the following section:

- Caveats in Cisco IOS XE 3.3S Releases, page 339

Caveats in Cisco IOS XE 3.3S Releases

Caveats describe unexpected behavior. 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 this chapter.

This section describes caveats in Cisco IOS XE 3.3S releases.

In this section, the following information is provided for each caveat:

- Symptom—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note: If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)
The Dictionary of Internetworking Terms and Acronyms contains definitions of acronyms that are not defined in this document:
http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

This section contains the following topics:
- Open Caveats—Cisco IOS XE Release 3.3.2S, page 340
- Resolved Caveats—Cisco IOS XE Release 3.3.2S, page 341
- Open Caveats—Cisco IOS XE Release 3.3.1S, page 350
- Resolved Caveats—Cisco IOS XE Release 3.3.1S, page 352
- Open Caveats—Cisco IOS XE Release 3.3.0S, page 359

### Open Caveats—Cisco IOS XE Release 3.3.2S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.3.2S.

- **CSCtr16465**
  - Symptoms: During Cisco IOS XE Release 3.2 to Cisco IOS XE Release 3.4 and Cisco IOS XE Release 3.3 to Cisco XE Release 3.4 ISSU upgrade or downgraded tests with MPLS features on both 4RU and 6RU, pending-issue is seen.
  - Conditions: This symptom occurs only MPLS features.
  - Workaround: There is no workaround.

- **CSCtr16637**
  - Symptoms: Active RP2 crashes.
  - Conditions: This symptom may occur while activating or deactivating billing over and over under 200 CPS NNI call and both XML and radius billing are enabled. This may result in check failure getting printed.
  - Workaround: There is no workaround.

- **CSCtr31773**
  - Symptoms: RP crashes.
  - Conditions: This symptom occurs with the following conditions:
    1. Header manipulate feature is enabled, and changes have been made.
    2. Switchover takes place.
  - Workaround: There is no workaround.

- **CSCtr38720**
  - Symptoms: Outbound calls fail due to code 47 error on Cisco ASR CUBE-ENT.
  - Conditions: Outbound calls fail on the Cisco ASR router due to an issue with the communication between the control and data plane of the Cisco ASR router.
  - Workaround: Reload the router.

- **CSCtr39816**
  - Symptoms: SBC crashes due to assert failure.
  - Conditions: SBC crashes when using Header Manipulation feature to do IP-FQDN for OPTION ping message. But when making a basic SIP call, the assert occurs and SBC crashes.
Workaround: There is no workaround.

- **CSCtr47472**
  Symptoms: Routes do not get added again after removing redistribute route-map.
  Conditions: This symptom occurs while using the following commands:
  - `Redistribute ospf 1 match internal ext 1 ext 2 route-map empty_map`
  - `No Redistribute ospf 1 match internal ext 1 ext 2 route-map map1`
  Workaround: There is no workaround.

- **CSCtr56484**
  Symptoms: Username attribute received in access-accept is not used by ISG as session-handle.
  Conditions: This symptom occurs when the username received by an ISG client needs to be over-written by contents of username (attribute1) response from Radius.
  Workaround: There is no workaround.

- **CSCtr56576**
  Symptoms: Cisco ASR router QFP crashes indicating either fragmentation or reassembly of packets.
  Conditions: This symptom occurs with QOS(service-policy) while using `set mpls experimental imposition` command in policy-map configuration.
  Workaround 1: Remove service-policy applied to the interface.
  Workaround 2: Downgrade to Cisco IOS Release 15.1(1)S2.

- **CSCtr65254**
  Symptoms: System core runs after 24, 48, and 72 hour traffic.
  Conditions: This symptom may occur after 24, 48, and 72 hour traffic.
  Workaround: There is no workaround.

- **CSCtr74460**
  Symptoms: Shutting down the GigabitEthernet0 interface on Cisco ASR1000 series routers with RP2 Route Processor card does not bring the link down. The LED of GigabitEthernet0 interface and the connected port on the switch are all in green.
  Conditions: This symptom occurs when a Cisco ASR1000 series router with RP2 Route Processor card is connected to a switch using GigabitEthernet0 interface.
  Workaround: There is no workaround.

### Resolved Caveats—Cisco IOS XE Release 3.3.2S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.3.2S.

- **CSCti98219**
  Symptoms: The router crashes upon transmission of MPLS-labeled packet.
  Conditions: This symptom is observed with Cisco IOS Release 12.4(24)T3 or Cisco IOS Release 15.0(1)M3. However, others may be affected. The router acts as an MPLS/VPN PE with VRF-NAT. This issue is seen when SIP packets are sent on the MPLS-facing interface.
  Workaround 1: Filter SIP traffic inbound on the IP-facing interface.
  Workaround 2: Configure “no ip nat service sip udp port 5060”.
- CSCtj14525
  Symptoms: Standby is not synced to active after attaching a new policy.
  Conditions: This symptom occurs when a dynamic policy is used such as RADIUS CoA.
  Workaround: There is no workaround.

- CSCtj30155
  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:
  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload
  Cisco has released free software updates that address these vulnerabilities.
  Workarounds that mitigate these vulnerabilities are available.

- CSCtk67768
  Symptoms: RP crash is observed in the DHCPD receive process.
  Conditions: This symptom occurs on the DHCP server that is used on Cisco ASR routers and acting as ISG.
  Workaround: There is no workaround.

- CSCtk69114
  Symptoms: RP resets while doing ESP reload with crypto configuration.
  Conditions: This symptom is observed by unconfiguring and configuring interface configuration and reloading both ESPs. The RP crashes on the server.
  Workaround: There is no workaround.

- CSCtl00995
  Symptoms: Cisco ASR 1000 series routers with 1000 or more DVTIs may reboot when a shut/no shut operation is performed on the tunnel interfaces or the tunnel source interfaces.
  Conditions: This symptom occurs when all the DVTIs have a single physical interface as the tunnel source.
  Workaround: Use a different tunnel source for each of the DVTIs. You can configure multiple loopback interfaces and use them as the tunnel source.

- CSCtn18784
  Symptoms: Interface Tunnel 0 constantly sends high bandwidth alarms.
  Conditions: The conditions are unknown at this time.
  Workaround: There is no workaround.

- CSCtn19027
  Symptoms: The show mediatrace responder sessions brief command crashes the router.
  Conditions: This symptom is observed on Mediatrace Responder when showing a stale session.
  Workaround: There is no workaround. Avoid issuing this impacted show command.
Caveats in Cisco IOS XE 3.3S Releases

- **CSCtn44232**
  Symptoms: With multiple RP switchovers, both RPs become unusable.
  Conditions: This symptom is observed with multiple RP switchovers.
  Workaround: There is no workaround.

- **CSCtn58128**
  Symptoms: BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.
  Conditions: This symptom may be triggered by route-flaps in a scaled scenario, where the route reflector may have 4000 route reflector clients and processing one million+ routes.
  Workaround: Ensure “no logging console” is configured.

- **CSCtn68117**
  Symptoms: Session command does not work on Cisco C3K series routers that have become the master after a mastership change.
  Conditions: This symptom is seen when failover to slave occurs.
  Workaround: There is no workaround.

- **CSCtn96521**
  Symptoms: When the Spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors fail to establish adjacency.
  Conditions: This symptom is observed when the Spoke (dynamic) peer group is configured before the iBGP (static) peer group.
  Workaround: If the order of creation is flipped, the two iBGP (static) neighbors will establish adjacency.

- **CSCtn97451**
  Symptoms: The bgp peer router crashes after executing the `clear bgp ipv4 unicast peer` command on the router.
  Conditions: This symptom occurs with the following conditions:

  Router3 ---ebgp--- Router1 ---ibgp--- Router2

  **ROUTER1:**

  -------
  interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
  ip pim sparse-mode
  !
  router ospf 100
  network 0.0.0.0 255.255.255.255 area 0
  !
  router bgp 1
  bgp log-neighbor-changes
  network 0.0.0.0
  neighbor 10.1.1.2 remote-as 1
  neighbor 10.1.1.3 remote-as 11
  !

  **ROUTER2:**

  -------
interface Ethernet0/0
  ip address 10.1.1.2 255.255.255.0
  ip pim sparse-mode
!
router ospf 100
  redistribute static
  network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
  bgp log-neighbor-changes
  network 0.0.0.0
  redistribute static
  neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4

ROUTER3:
--------
interface Ethernet0/0
  ip address 10.1.1.3 255.255.255.0
  ip pim sparse-mode
!
router bgp 11
  bgp log-neighbor-changes
  network 0.0.0.0
  network 0.0.0.0 mask 255.255.255.0
  redistribute static
  neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4

Crash reproduce steps are as follows:
1. Traffic travel from ROUTER3 to ROUTER2.
2. “clear bgp ipv4 unicast 10.1.1.1” on ROUTER2.

Workaround: There is no workaround.

- CSCto00796
  Symptoms: In a rare and still unreproducible case, the RR (also PE) misses sending the RT extended community for one of the redistributed VPNv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR).
  Conditions: This symptom occurs when a new interface is provisioned inside a VRF and the configuration such that the connected routes are redistributed in the VRF. This redistributed route fails to tag itself with the RT when it reaches the peering PE (+RR)
  Workaround: Soft clear the peer that missed getting the RT.

- CSCto07586
  Symptoms: An IPV4 static BFD session does not get established on a system which does not have IPV6 enabled.
  Conditions: This symptom occurs with the following conditions:
  1. Create an IOS image that does not have IPV6 enabled.
  2. Enable BFD on an interface.
  3. Configure an IPV4 static route with BFD routing through the above interface.
The IPV4 BFD session does not get established, so the static route does not get installed.
Workaround: Unconfigure BFD on the interface, and then reconfigure it. Then, the session will come up.

- **CSCto07919**
Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:
  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload
Cisco has released free software updates that address these vulnerabilities.
Workarounds that mitigate these vulnerabilities are available.

- **CSCto16106**
Symptoms: Address is not assigned when “ip dhcp use class aaa” is configured.
Conditions: When the DHCP server is configured to download a class name from the radius using “ip dhcp use class aaa” and lease an IP address from that class, the IP address is not assigned to the client.
Workaround: There is no workaround.

- **CSCto31265**
Symptoms: ABR does not translate Type7 when primary Type7 is deleted even if another Type7 LSA is available.
Conditions: This symptom occurs with OSPFv3. ABR receives multiple Type7 LSA for the same prefix from Multiple ASBR.
Workaround 1: Delete/readd the static route that generates Type7.
Workaround 2: Execute the `clear ipv6 ospf force-spf` command on ABR.
Workaround 3: Execute the `clear ipv6 ospf redistribution` command on ASBR.

- **CSCto35160**
Symptoms: After switchover, traffic drops are seen in CARRIER-Ethernet testcase for about 15 seconds. This issue is not seen consistently.
Conditions: This symptom is seen after switchover.
Workaround: It will auto restore after 15 seconds.

- **CSCto41165**
Symptoms: The standby router reloads when you use the `ip extcommunity-list 55 permit|deny` command, and then the `no ip extcommunity-list 55 permit|deny` command.
Conditions: This symptom occurs when the standby router is configured.
Workaround: There is no workaround.

- **CSCto41223**
Symptoms: The standby IOSD crashes when standby RP reload is executed.
Conditions: This symptom is observed in a scaled configuration with 8000 EoMPLS and 8000 EVC sessions while the traffic is flowing. On issuing standby RP reload, IOSD crashes at the process “Standby service handler”.

Workaround: There is no workaround.

- CSCto46716
  Symptoms: Routes over the MPLS TE tunnel are not present in the routing table.
  Conditions: This symptom occurs when the MPLS TE tunnel is configured with forwarding adjacency. In “debug ip ospf spf”, when the SPF process link for the TE tunnel is in its own RTR LSA, the “Add path fails: no output interface” message is displayed. Note that not all tunnels are affected. It is unpredictable which tunnel is affected, but the number of affected tunnels grows with the number of configured tunnels.
  Workaround: If feasible, use autoroute announce instead of forwarding adjacency. Otherwise, upgrade to the fixed version.

- CSCto55643
  Symptoms: High CPU loading conditions can result in delayed download of multicast routes to line cards, resulting in multicast forwarding (MFIB) state on line cards out of sync with the RP. The `show mfib linecard` command shows line cards in sync fail state with many in LOADED state.
  Conditions: This symptom occurs during high CPU loading due to router reload or line card OIR events in a highly scaled multicast environment with high line rates of multicast traffic and unrestricted processed switched packets, before HW forwarding can be programmed.
  Workaround: There is no workaround. Ensure that mls rate limits are properly configured.
  Further Problem Description: IPC errors may be reported in the MRIB Proxy communications channel that downloads multicast routes to line cards.

- CSCto55983
  Symptoms: After reload, incoming mcast traffic is sent into the CPU before MFIB is downloaded into line cards. Due to the high CPU rate, line cards are stuck in a continual loop of failing to complete MFIB download and retrying.
  Conditions: This symptom occurs during high CPU utilization caused by multicast traffic. The `show mfib line summary` command does not show cards in sync.
  Workaround: There is no workaround.

- CSCto69071
  Symptoms: Metrics collection fails due to invalid DVMC runtime object handle.
  Conditions: This symptom occurs when the transport layer is not passing up an interface type that is acceptable to DVMC.
  Workaround: There is no workaround.

- CSCto72480
  Symptoms: The output of the `show mfib linecard` command shows that line cards are in “sync fail” state.
  Conditions: This symptom occurs usually when the last reload context displayed in the `show mfib linecard internal` command output is “epoch change”. This indicates that an IPC timeout error has occurred in the MRIB communications channel that downloads multicast routing entries to the multicast forwarding information base (MFIB). In this condition, multicast routing changes are not communicated to the failed line cards and they are not in sync with the RP.
Workaround: If this issue is seen, using the `clear mfib linecard slot` command may clear the problem. If the problem occurs on a Cisco 7600 SP, an RP switchover is required after clearing the problem on any affected line cards. The workaround may not completely work if high CPU loading continues to be present and IPC errors are reported.

Further Problem Description: The IPC timeout errors could result from high CPU loading conditions caused by high rates of processed switched packets. High rates of multicast processed switched packets can be avoided if rate limits are applied after each router boot, especially after using the `mls rate-limit multicast ipv4 fib-miss` command.

- **CSCto76018**
  Symptoms: The Cisco ASR1000-WATCHDOG process crashes on DVTI Server after clearing crypto session on DVTI Client.
  Conditions: This symptom occurs for sessions with the configuration of 1000 VRFs, 1 IKE session per VRF, and 4 IPSec SA dual per session. The Cisco ASR1000-WATCHDOG process crashes on the DVTI Server during clear crypto session on the DVTI client, after all the SAAs have been established.
  Workaround: There is no workaround.

- **CSCto88581**
  Symptoms: The standby RP crashes following an interface configuration change.
  Conditions: This symptom is observed only when “ospf non-stop routing” is configured.
  Workaround: There is no workaround.

- **CSCto90252**
  Symptoms: A standby route processor (RP) is stuck to “init, standby” for about 10 hours.
  Conditions: This symptom occurs after reloading five or six times on a Cisco ASR 1000 series router.
  Workaround: Disable NSR.

- **CSCto98212**
  Symptoms: The IPv6 address and prefix 2001:DB8:1:104::/64 at 25 Aug 2011 00:01 25 Jul 2011 00:01 are lost after a router realod.
  Conditions: This symptom occurs when this command checks for the clock validity. When the router reloads the clock validity is displayed as “not yet valid”. This causes the command to not be applied.
  Workaround: There is no workaround.

- **CSCto99523**
  Symptoms: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR).
  Conditions: This symptom occurs when convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR). There is no functionality impact.
  Workaround: There is no workaround.

- **CSCtq04117**
  Symptoms: DUT and RTRA have a IBGP-VPNv4 connection that is established via loopback. OSPF provides reachability to a BGP next hop, and BFD is running.
  Conditions: This symptom occurs under the following conditions:
  1. DUT has learned VPNv4 route from RTRA, and the same RD import is done at DUT.
2. When switchover is performed in RTRA and when GR processing is done, the route is never imported to VRF.

Workaround: Use the `clear ip route vrf x *` command.

- **CSCtq06538**

  Symptoms: The RP crashes due to bad chunk in MallocLite.

  Conditions: This symptom occurs while executing testcase number 4883. The test case 4883 sends an incorrect BGP update to the router to test whether the router is able to handle the problematic update. The incorrect BGP update has the local preference attribute length incorrect:

  ```
  LOCAL_PREF
  Header
  AttributeFlags
  Optional: 0b0
  Transitive: 0b1
  Partial: 0b0
  ExtendedLength: 0b0
  Unused: 0b0 0b0 0b0 0b0
  TypeCode: 0x05
  Length: 0x01 <----- should be 0x04 instead
  Value: 0xff 0xff 0xff 0xff
  NetworkLayerReachabilityInfo: 0x08 0x0a <snip>
  ```

  Workaround: There is no workaround.

- **CSCtq22873**

  Symptoms: The router may show the following traceback (error message) after receiving certain IPv6 packets:

  ```
  TB:%SCHED-2-EDISMSCRIT:process=PuntInject Keepalive Process
  ```

  Conditions: This symptom when the router is configured for IPv6 routing.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.


- **CSCtq23793**

  Symptoms: After reloading the PE router in the mVPN network, multicast traffic stops on one of the VRFs randomly.

  Conditions: This symptom occurs under the following conditions:
  - When reloading a PE in mVPN network.
  - When PE has many VRFs and scaled mVPN configuration.

  Workaround: Remove and add the MDT configuration.

- **CSCtq32896**

  Symptoms: LSM entries stop forwarding traffic.

  Conditions: This symptom is observed after Stateful Switchover (SSO).

  Workaround: There is no workaround.
Caveats in Cisco IOS XE 3.3S Releases

- CSCtq43480  
  Symptoms: A Cisco router crashes.  
  Conditions: This symptom occurs when a session starts with PBHK and accounting features while the method list is not provisioned for the accounting features.  
  Workaround: There is no workaround.

- CSCtq46745  
  Symptoms: Custom configured default sip profiles (option/method/header) are lost during a router reload.  
  Conditions: This symptom occurs during reload.  
  Workaround: Use non-default profiles for each adjacency.

- CSCtq46760  
  Symptoms: When doing ISSU subpackage upgrade from Cisco IOS XE Release 3.2.2 to Cisco IOS XE Release 3.4.0 with the Cisco IOS XE Release 2.3 feature set, both FPs crash and multiple core files are seen after the last ISSU step, active RP loadversion.  
  Conditions: This symptom only occurs on Cisco ASR1006 subpackage upgrade with dual RPs.  
  Workaround: Reload the standby RP before switchover.

- CSCtq56078  
  Symptoms: Performance downgrade occurs after 8k SDP support.  
  Conditions: This symptom occurs after SBC rejects the call if SDP is over 5k.  
  Workaround: There is no workaround.

- CSCtq62759  
  Symptoms: The CLNS routing table is not updated when the LAN interface with the CLNS router ISIS configured shuts down because ISIS LSP is not regenerated. The CLNS route will be cleared after 10 minutes when ISIS ages out the stale routes.  
  Conditions: This symptom is seen when only the CLNS router ISIS is enabled on the LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.  
  Workaround: Use the `clear clns route` command or the `clear isis *` command.

- CSCtq83629  
  Symptoms: The error message is associated with a loss in multicast forwarding state on line cards under scaled conditions when an IPC error has occurred.  
  Conditions: This symptom is observed during router boot or high CPU loading, which can cause IPC timeout errors. This issue is seen on line cards during recovery from an IPC error in the MRIB channel.  
  Workaround: Line card reload is required to resolve the problem.

- CSCtq92182  
  Symptoms: An eBGP session is not established.  
  Conditions: This issue is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.  
  Workaround: Use an IPv6 neighbor address with bits. Set some higher bits, along with the IPv4 mapped address.
• CSCtq96329
  Symptoms: Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.
  Conditions: This symptom can happen only when bgp deterministic-med is configured.
  The following releases are impacted:
  – Cisco IOS Release 15.0(1)S4
  – Cisco IOS Release 15.1(2)T4
  – Cisco IOS Release 15.1(3)S
  – Cisco IOS Release 15.2(1)T
  Workaround: Disable deterministic med in the network/AS by issuing the no bgp deterministic-med command and then the clear ip bgp* command or hardreset of BGP session to remove any stale prefixes.

• CSCtr07704
  Symptoms: While using scripts to delete nonexistent classmap filter from a class, the router sometimes crashes (c2600XM) or returns traceback spurious memory access (c2801nm).
  Conditions: This symptom occurs when trying to delete a nonexistent classmap filter, the classmap will be NULL, and passed to match_class_params_same. This results in referencing a null pointer.
  Workaround: Do null check in match_class_command and match_class_params_same. To keep the existing behavior, do not print out a message like “the class does not exist” when deleting a nonexistent class map from a class.

• CSCtr30820
  Symptoms: The IP address is not assigned to the client after a DHCP request.
  Conditions: The problem is observed while verifying the VRF-aware-DHCP functionality in Cisco IOS relay and server in an MPLS setup.
  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.3.1S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.3.1S.

• CSCtq46745
  Symptom: Default SIP profiles (option, method, or header) that were custom configured earlier are lost during a router reload.
  Conditions: This issue is observed when a router is reloaded.
  Workaround: Use nondefault profiles for each adjacency.

• CSCtq36726
  Symptom: Configuring ip nat inside command on the IPSEC dVTI VTEMP interface does not have any effect on the cloned virtual-access interface. The NAT functionality is thus broken, because the virtual-access interfaces does not get this command cloned from the respective VTEMP.
  Conditions: This issue occurs on the Cisco ASR1006 (RP2/FP20) Router, with IKEv2 dVTI, and the router running Cisco IOS XE 3.4 throttle builds. This could be service impacting and easily reproducible.
Workaround: Reconfigure the virtual-access interface such that the `ip nat inside` command is configured first, followed by the other commands.

- **CSCtj94589**
  Symptom: The Cisco ASR 1000 Router crashes when a testbed is unconfigured.
  Conditions: This issue is observed when you perform the following procedure:
  1. Configure 1000 VRF (`vrf!=ivrf`).
  2. Configure one IKE session per VRF.
  3. Configure four SA duals per session.
  4. Unconfigure the testbed when the IXIA traffic ends.
  The Cisco ASR 1000 Router may crash when the `no vrf vrf-name` command is issued under the `crypto isakmp` profile.
  Workaround: There is no workaround.

- **CSCtk69114**
  Symptom: The RP resets when performing ESP reload, which includes crypto configuration.
  Conditions: This issue is observed when you perform the following procedure:
  1. Unconfigure and configure the interface configuration.
  2. Reload both the ESPs.
  The RP crashes on the server at the end of this procedure.
  Workaround: There is no workaround.

- **CSCtl92842**
  Symptom: The Cisco ASR1000 Router crashes in the controller-config mode.
  Conditions: This issue is observed when SPA-CHOC3-CE-ATM is removed and configured in the controller config mode (`config-controller`).
  Workaround: Exit the controller config (`config-controller`) mode before removing the SPA.

- **CSCtn28194**
  Symptom: When the virtual CEM interface is disabled, it drops out-of-band clocking packets, after an RP switchover.
  Conditions: This issue is observed when RP switchover is performed with out-of-band clocking.
  Workaround: If the network clock status changes after the standby RP is booted, execute the `shut` and `no shut` commands on the virtual CEM circuit.

- **CSCtn55892**
  Symptom: The CEM interface status is shown as Down on a Cisco ASR1000 Router.
  Conditions: This issue is observed upon configuring CESoPSN or the SAToP circuit on a freshly booted router. However, the traffic flow is not affected despite the CEM interface status being Down.
  Workaround: Execute the `shut` and `no shut` commands on the CEM interface in order to bring the interface up.

- **CSCto09829**
  Symptom: The standby ESP crashes intermittently, with FTP traffic generating a core and throwing tracebacks on the console.
Caveats in Cisco IOS XE 3.3S Releases

Conditions: This issue is observed when the WCCP is configured along with the firewall and the FTP traffic is running.
Workaround: There is no workaround.

- CSCto16196
  Symptom: Unconfiguring and reconfiguring of WCCP tunnels results in tracebacks. The tracebacks are accompanied by partial or full traffic loss.
  Conditions: This issue is seen on the routers that have the WCCP and PFR features enabled. Reapplying the WCCP after WCCP tunnels are configured and unconfigured, causes this issue.
  Workaround: There is no workaround.

- CSCto32753
  Symptom: Unconfiguring and reconfiguring of WCCP tunnels results in tracebacks. The tracebacks are accompanied by partial or full traffic loss.
  Conditions: This issue is seen on the routers that have the WCCP and PFR features enabled. Reapplying the WCCP after WCCP tunnels are configured and unconfigured, causes this issue.
  Workaround: There is no workaround.

- CSCto76009
  Symptom: The old IPSec SAs cannot be removed after the DVTI client is reloaded.
  Conditions: This issue is observed when you establish 8000 IPSec SAs using the DVTI server-client mechanism. When you reload the DVTI client a couple of times, with a reload time interval of 10 minutes, the number of IPSec SAs on the DVTI server increases above 10000 and soon approaches 20000, crossing the SAs limit of 8000.
  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.3.1S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.3.1S.

- CSCtn71898
  Symptom: During an ISSU subpackage upgrade from Release 3.2.x to Release 3.3.0, the router crashes. During an ISSU subpackage downgrade from Release 3.3.0 to Release 3.2.x, the standby RP does not come up correctly after the procedure. Instead, the standby RP reloads continuously and IPC timeout messages are generated each time the RP reloads.
  Conditions: These issues are observed when ISSU subpackage upgrade is performed on the router.
  Workaround: There is no workaround.

- CSCth52252
  Symptom: When more than one EzVPN clients initiate a connection to the dVTI EzVPN server using the same NAT device, the first client connects to the server. But when the second client connects to the server, traffic passes through the second client, but fails on the first client.
  Conditions: This issue is observed when more than one EzVPN clients initiate sessions to the dVTI EzVPN server using the same NAT device.
Workaround: There is no workaround.

- **CSCtj46670**
  Symptoms: The IPCP cannot be completed after the dialer interface has moved out of the Standby mode. CONFRERJ is seen while negotiating the IPCP.
  Conditions: This symptom is observed when the dialer interface has moved out of the Standby mode. When a dialer debugs is enabled, the `DDR: Cannot place call, no dialer string set` error message is displayed.
  Workaround: Reload the router.

- **CSCtj55624**
  Symptoms: The Cisco ASR 1000 Router crashes when the `show crypto ruleset` command is run.
  Conditions: This issue is observed when the v6 crypto maps are configured.
  Workaround: Do not run the `show crypto ruleset` command.

- **CSCtj78966**
  Symptoms: The Cisco ASR 1000 Router crashes if many operations of IKEv2 sessions are open.
  Conditions: This symptom is seen when the IKEv2 SA DB WAVL tree gets corrupted after the SA insertion failure occurs, for example, during the PSH duplication.
  Workaround: There is no workaround.

- **CSCtj87846**
  Symptoms: The Performance Routing (PfR) traffic class fails to transition out of the default state.
  Conditions: This issue occurs when a subinterface is used as an external interface and the corresponding physical interface goes down and comes up. The PfR master is not notified that the subinterface is up.
  Workaround: Execute the `shut` or `no shut` commands on both the PfR master and PfR border.

- **CSCtj91149**
  Symptoms: After the dynamic XConnect-based ISG session is up on the active RP, a delay of approximately 30 seconds is observed for the dynamic XConnect-based ISG session to be up on the standby RP.
  Conditions: This symptom occurs on switchover.
  Workaround: There is no workaround.

- **CSCtj94510**
  Symptoms: When sessions are being set up with the configuration of 1000 VRFs (fvrf!=ivrf)—one IKE session per VRF and four SA duals per session—a crash occurs during the Crypto_SS_process.
  Conditions: This symptom occurs when sessions are being set up with the configuration of 1000 VRFs (fvrf!=ivrf)—one IKE session per VRF and four SA duals per session.
  Workaround: There is no workaround.

- **CSCtk46381**
  Symptoms: Service policy installation on the L2transport PVP fails when the shaping rate is changed.
  Conditions: This issue occurs when the PVPs shaping rate of the PVPs is changed.
  Workaround: Remove and reinclude the service policy.
- **CSCtk83638**
  Symptoms: An IP address from an incorrect pool is assigned to a client when the client reconnects with a different pool of IP addresses.
  Conditions: This issue is observed in a setup where two clients are behind a NAT router. This occurs when one client’s connection is broken and the server is not aware of it, and the client reconnects with a different group and the IP address that is assigned is not from the correct pool.
  Workaround: There is no workaround.

- **CSCtl70143**
  Symptoms: Sometimes, the Broadband L2TP Access Concentrator (LAC) does not forward a Point-to-Point-Protocol (PPP) CHAP-SUCCESS message from the L2TP Network Server (LNS) to a client.
  Conditions: This issue occurs when a T1(PRI) is used between a client and the LAC.
  Workaround: There is no workaround.

- **CSCtl78285**
  Symptoms: In a VRF configuration, an RD cannot be deleted after the RD configuration is deleted.
  Conditions: This occurs when the VRF is configured with the RD.
  Workaround: Remove the VRF configuration and add the VRF again.

- **CSCtl84797**
  Symptoms: An SBC traceback occurs.
  Conditions: This issue is observed when Lawful Intercept (LI) is enabled, and multiple media sessions are present in a single call. (SDP contains information about multiple media sessions.)
  Workaround: There is no workaround.

- **CSCtl98535**
  Symptoms: The "FMANRP_CEF-4-UPDSTATSERR: Update CEF statistics error" traceback error message is displayed when different images are running in the active and standby RPs.
  Conditions: This occurs when different Cisco IOS software images are running in the active and standby RPs.
  Workaround: There is no workaround.

- **CSCtl99266**
  Symptoms: 1) CoA service login is not synchronized to the standby RP. 2) CoA multiservice login and logout are not synchronized to the standby RP.
  Conditions: The first issue occurs when a CoA service logout that was not installed through CoA service login (that is installed through a rule or as an auto service) takes place. The configuration gets synced to standby. When you perform a CoA service login of the same service.
  The second issue occurs when you perform a CoA multiservice login and logout of more than one service takes place. The services are applied or unapplied on an active RP, but not on a standby RP.
  Workaround: For the first issue, if the CoA service login is not synchronized, reboot the standby RP. After the standby RP comes up, initiate a bulk synchronization from the active RP. This synchronizes the service login. For the second issue, there is no workaround.
- **CSCtn19444**
  Symptoms: Both the mLACP PoAs may bundle their memberlinks, resulting in both the PoAs becoming active.
  Conditions: This issue occurs when running mLACP. The ICRM connection between the PoAs is lost. If the interface that is configured as the backbone interface also goes down on one of the PoAs, that PoA might keep its port channel memberlinks bundled. The end result is that both the PoAs are in the mLACP active state, and both have their port channel memberlinks bundled.
  Workaround: Configure shared control by configuring lacp max-bundle on the Dual Homed Device (DHD) if the device supports it. This prevents the DHD from bundling the memberlinks to both the PoAs at the same time.

- **CSCtn38996**
  Symptoms: All MVPN traffic gets blackholed when a peer is reachable using a Traffic Engineering (TE) tunnel. Although an interface flap is performed so that a secondary path can be selected, the multicast route does not contain a native path that uses the physical interface.
  Conditions: This issue occurs when MPLS traffic-eng multicast-intact is configured under OSPF.
  Workaround: Execute the `clear ip ospf process` command on the core router.

- **CSCtn39632**
  Symptoms: The RSA key cannot be configured under a key ring. It can be configured only in the global configuration.
  Conditions: This issue occurs on a Cisco ASR 1000 Series Router that is configured for RSA key encryption, with the key ring name having more than eight characters.
  Workaround: Modify the key ring name such that it is less than eight characters.

- **CSCtn42601**
  Symptoms: The Cisco router may unexpectedly reload when OSPF event debugging is enabled.
  Conditions: This issue is observed when you perform the following procedure:
  1. Configure the OSPF router to redistribute another protocol, with redistribution being controlled by a route map.
  2. Enable the `debug ip ospf events` command.
  Workaround: Do not reconfigure route maps when OSPF event debugging is in progress. Disable OSPF event debugging before making configuration changes to the route map.

- **CSCtn46263**
  Symptoms: Memory leaks are seen in ikev2_packet_enqueue and ikev2_hash.
  Conditions: This symptom is observed during retransmissions and window throttling of requests.
  Workaround: There is no workaround.

- **CSCtn51058**
  Symptoms: Traffic drops lead to long multicast reconvergence periods.
  Conditions: This issue is observed when stateful switchover (SSO) is performed.
  Workaround: There is no workaround.

- **CSCtn51740**
  Symptoms: Memory leak is observed during the EzVPN process.
Conditions: This symptom is seen when an EzVPN connection is configured with split tunnel attributes.

Workaround: There is no workaround.

- CSCn56526
Symptoms: In the current Cisco IOS XE 3.2.0 software, MBS is calculated based only on the MTU value. User-defined MBS value that can be calculated using the `show atm pvc` command is not displayed.

Conditions: This issue is observed when you perform the following procedure:
  1. Configure the MBS from the command-line interface (CLI).
  2. Check the `show atm pvc` command output.

The MBS does not reflect the configured value. It's value is always based on MTU size.

Workaround: There is no workaround.

- CSCn61834
Symptoms: The NAT-T keepalive configuration is unable to send the cause for the NAT translation timeout.

Conditions: The NAT translation table is getting timed out, because no NAT keepalive message is received.

Workaround: There is no workaround.

- CSCn64500
Symptoms: Multicast traffic does not pass through an ATM point to a multipoint subinterface.

Conditions: This issue is caused because of an incomplete inject P2MP multicast adjacency on the ATM P2MP interface. The output of the `show adjacency ATM interface detail` command shows that the inject P2MP multicast adjacency is in an incomplete state.

Workaround: Execute the `clear adjacency` command to force the repopulation of the incomplete adjacency. You should be aware of the impact of this system-wide command. Alternatively, you can use unicast commutation if it is possible to do so.

- CSCn73941
Symptoms: After performing an OIR for an ES+ card having EVC configuration with the `module clear-config` command, performing a restore of the old configuration is no longer functional, indicating that traffic will not be forwarded over to those service instances. The VLANs used in the previous configuration cannot be effectively used on the ports, even if the service instance numbers are changed.

Conditions: This symptom occurs when the `module clear-config` command is configured.

Workaround: There is no workaround.

- CSCn74169
Symptoms: The router crashes because of the memory corruption that occurs with the use of the EzVPN Web-intercept daemon process.

Conditions: This issue is observed when the EzVPN connection comes up after HTTP authentication is completed with the help of the HTTP intercept.

Workaround: HTTP intercept should not be used.

- CSCn80993
Symptoms: After performing an OIR of a SPA, the Cisco IOS crashes.
Conditions: This issue is observed when you perform the following procedure:
1. The router has scaled the L2VPN configuration of 7000 EoMPLS.
2. The router is configured with 1500 TE tunnels, 6000 EVC, and 3000 L2TPv3 sessions.
3. A SPA OIR is performed, when the traffic is passing through the sessions.

The Cisco IOS crashes consistently after these configuration steps are performed.
Workaround: After the SPA comes up, wait for 1 minute before issuing the second reload.

- **CSCtn81231**
  Symptoms: Multicast traffic is not forwarded out of the RBE interface because of incomplete multicast adjacency.
  Conditions: This issue is observed when you perform the following procedure:
  1. An ATM DCHP host running IGMPv2 is established over the RBE interface of the router.
  2. Multicast group join configuration is successful.
  However, multicast adjacency is incomplete and hence cannot forward multicast traffic.
  Workaround: Execute the `shut` command followed by the `no shut` command on the ATM main interface.

- **CSCtn87155**
  Symptoms: The CoA sessions do not come up.
  Conditions: This symptom is seen when some CLI commands are called within the shell function.
  The CLI commands may fail if the shell programatic APIs are used.
  Workaround: Manually use the shell function on the console.

- **CSCtn98642**
  Symptoms: The ASR RP crashes with the: UNIX-EXT-SIGNAL: Segmentation fault(11),
  Process = Ether-SPA background process error message.
  Conditions: This issue is observed when you perform the following configurations:
  1. Perform a large-scale configuration having QinQ and QinQ-Any with the same outer VLAN on
     the SPA.
  2. Reload the router.
  Workaround: There is no workaround.

- **CSCto00318**
  Symptoms: Performing an SSH on an existing SSH session causes the router to reboot at times.
  Conditions: This issue is observed when an intermediate server is an IOS server. An SSH session
  initiated from a router running Cisco IOS Release 15.x IOS may cause the router to reboot. Do not
  initiate an SSH session from the Cisco router running the Cisco IOS 15.x IOS release train.
  Workaround: There is no workaround.

- **CSCto02448**
  Symptoms: The AS Path attribute is lost when performing an inbound route refresh.

---

**Note**
Configuration of QinQ (min 50) and QinQ-Any with the same outer VLAN is mandatory.
Conditions: This symptom is observed when you perform the following procedure:

1. Configure the neighbor with soft reconfiguration inbound.
2. Do not configure the inbound route map for the neighbor router.

The nonroute map inbound policy (filter-list) allows the AS path.

Workaround: Instead of using the nonroute map inbound policy, use the route map inbound policy to filter the prefixes.

- CSCto03123
  Symptoms:
  1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
  2. Additional memory leak can occur when frequent sensor value changes take place.

   Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.

   Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

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

- CSCto44585
  Symptoms: Packets with the DF-bit set across the L2TPV3 tunnel are punted or dropped into the CPU.

  Conditions: This symptom occurs when the PMTU in the pseudowire class configuration is enabled.

  Workaround: Reduce the size of the MTU on the client side.

- CSCto48592
  Symptoms: The IPFRR: IOS crashes when switchover is performed.

  Conditions: This issue is observed when you perform the following procedure:
  1. Enable IPFRR.
  2. Enable BFD.
  3. Perform a switchover to the active RP.

  Workaround: There is no workaround.

- CSCto52235
  Symptoms: The mac address accounting command is missing in the Cisco ASR 1000 Router.

  Conditions: Not applicable.

  Workaround: There is no workaround.

- CSCto63954
  Symptoms: The router crashes continuously, if GETVPN is configured in the router.

  Conditions: This symptom occurs when GETVPN-related configuration is performed in the router.
Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.3.0S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.3.0S.

- CSCti53718
  Symptom: While performing a consolidated package upgrade on the Cisco ASR 1006 Router, the standby ESP does not proceed beyond the Init state.
  Conditions: This issue is observed in active PPPoEoA sessions when a create-on-demand VC with no PPP keepalive is configured and QoS is configured at the BB session level.
  Workaround: Configure a PPP keepalive.

- CSCto03123
  Symptoms:
  1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
  2. Additional memory leak can occur when frequent sensor value changes take place.
  Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.
  Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
Caveats in Cisco IOS XE 3.3S Releases

- **CSCtj31320**
  
  **Symptom:** MLP bundles miss adjacencies after a scaled configuration router is reloaded. The bundles either do not process traffic or process only traffic that is forwarded in one direction. When the `show ip route` command is run, the output indicates that there is no adjacency entry for the peer IP address.

  **Conditions:** This issue is observed after the router is reloaded, a hardware OIR is performed, an interface flaps, or some other event that causes a large number of MLP bundle sessions to be terminated and re-established occurs.

  **Workaround:** For MLP over Serial interfaces, perform one of the following actions on the bundle:
  - Run the `clear interface bundle_interface_name` command.
  - Shut down, and then restart the bundle.

  For MLPPPoE interfaces, run the `clear interface bundle_interface_name` command.

  The bundle may recover after you perform one of these actions. In addition, to avoid this issue if flaps occur in the future, implement the following combination of PPP and multilink options:
  - `ppp timeout retry 4`
  - `ppp max-failure 30`
  - `ppp multilink ncp sequenced never`

- **CSCtk03524**
  
  **Symptom:** Applying a single dynamic crypto map to a large number (for example, 2000) of subinterfaces while the crypto session is being set up causes the `iosd check heap coredump` error.

  **Conditions:** This issue is observed when a large number of subinterfaces share a single dynamic crypto map.

  **Workaround:** Configure each subinterface to use a different crypto map.

- **CSCtk10772**
  
  **Symptom:** The LNS CPS rate is reduced for PPP/VPDN sessions.

  **Conditions:** This issue is observed when LNS is configured with dual RP in SSO High Availability mode. The LNS CPS rate is reduced when the session count exceeds 16000 PPP/VPDN sessions.

  **Workaround:** Disable SNMP on the virtual-template by running the `no virtual-template snmp` command.

- **CSCtk69937**
  
  **Symptom:** Packets may get dropped during the IPSec rekey process in an IKEv2 session.

  **Conditions:** This issue is observed during the IPSec rekey process in an IKEv2 session.

  **Workaround:** There is no workaround.

- **CSCt71869**
  
  **Symptom:** A traceback is seen when the `default interface` command is run using a script to clean up the configuration on the interface.

  **Conditions:** This issue is observed when an Ethernet service instance (that is, the EFP) is configured on the interface.

  **Workaround:** Manually run the `default interface` command. If you want to include the command in a script, then add a delay in the script before the command is run.

- **CSCt92842**
Symptom: The router crashes if SPA-CHOC3-CE-ATM is removed while the router is being configured in the Controller Configuration mode.

Conditions: This issue is observed when SPA-CHOC3-CE-ATM is removed while the router is being configured in the Controller Configuration mode.

Workaround: Exit the Controller Configuration mode before removing the SPA.

- **CSCtl95778**

  Symptom: BBA traffic is dropped on the standby RP while an ISSU upgrade from Cisco IOS XE Release 3.1.x or 3.2.x to 3.3.0 is in progress. In addition, L2TPv3 traffic is lost and cannot be recovered after the ISSU is completed.

  Conditions: This issue is observed when an ISSU is performed from Cisco IOS XE Release 3.1.x or 3.2.x to 3.3.0.

  Workaround: Manually reload the standby RP before the final RP switchover.

- **CSCtl99266**

  Symptom: The following issues related to CoA services are observed:
  - CoA service activation details are not propagated from the active RP to the standby RP.
  - CoA multiservice activation or deactivation of multiple services is not propagated from the active RP to the standby RP.

  Conditions: The first issue is observed when the following steps are performed:

  1. Perform a CoA service deactivation of a service that was not installed though CoA service activation (that is, it was installed through a rule or as an auto service). The deactivation details are propagated to the standby RP.
  2. Perform a CoA service activation of the same service. The activation details are not propagated to the standby RP.

  Workaround: For the first issue, reboot the standby RP. There is no workaround for the issue related to CoA multiservice activation or deactivation.

- **CSCtn00790**

  Symptom: PPPoEoA sessions are not automatically re-established after an RP switchover.

  Conditions: This issue is observed when ISG is configured.

  Workaround: There is no workaround.

- **CSCtn28194**

  Symptom: After an RP switchover, the virtual-cem interface is disabled and drops out-of-band clocking packets.

  Conditions: This issue is observed when an RP switchover is performed with out-of-band clocking.

  Workaround: If the network clock status changes after the standby RP is started, shut down and then restart the virtual-cem circuit.

- **CSCtn28453**

  Symptom: The virtual-cem interface remains in the down/down state. This results in packets getting dropped because of input errors.

  Conditions: This issue is observed when system is configured as the source of the network clock by using the network-clock select priority system command and is selected as the active source, but is not selected for CEM out-of-band clocking.

  Workaround: There is no workaround.
• CSCtn31692
  Symptom: After an RP switchover, the BITS clock is not selected as the ACTIVE clock source. Instead, the system clock is selected as the ACTIVE clock source.
  Conditions: This issue is observed when a valid BITS clock source is connected to R0 or R1, the network clock is configured using the network-clock select priority BITS R0/R1 command to select BITS input from R0 or R1, and an RP switchover is performed.
  Workaround: There is no workaround.

• CSCtn43861
  Symptom: When the parameterized L4R-Whitelist combo service is applied, incoming packets matching the whitelist may still get redirected. In addition, explicit traffic priorities configured in the service template are not inherited by the parameterized service policy. When the show subscriber session uid uid is run, the priorities configured for the services are not correctly displayed.
  Conditions: This issue is observed when the show subscriber session uid uid command is run. However, note that after explicitly applying a priority to the parameterized L4R and the whitelist TCs, if you try service activation either through Access-Accept or CoA, the sessions come up and the services are activated.
  Workaround: There is no workaround.

• CSCtn44232
  Symptom: When multiple RP switchovers are performed, a stage may be reached where both RPs are unusable.
  Conditions: This issue is observed when multiple RP switchovers are performed.
  Workaround: There is no workaround.

• CSCtn55892
  Symptom: The CEM interface is in the down/down state.
  Conditions: This issue is observed when you configure a CESoPSN or SAToP circuit on a recently booted router. Note that traffic flow is not affected because of this issue.
  Workaround: Shut down, and then restart the CEM interface.

• CSCtn62287
  Symptom: The standby RP may crash while flapping the interface or performing a soft OIR of the SPA.
  Conditions: This issue is observed when interfaces are bundled as a multilink and traffic is flowing across the multilink.
  Workaround: There is no workaround.
Caveats in Cisco IOS XE 3.2S Releases

This chapter provides information about caveats in Cisco IOS XE 3.2S releases. Because Cisco IOS XE 3S is based on Cisco IOS XE 2 inherited releases, some caveats that apply to Cisco IOS XE 2 releases also apply to Cisco IOS XE 3S. For a list of the software caveats that apply to Cisco IOS XE 2, see the “Caveats for Cisco IOS XE Release 2” section at the following location:

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

This chapter contains the following section:

- Caveats in Cisco IOS XE 3.2S Releases, page 363

Caveats in Cisco IOS XE 3.2S Releases

Caveats describe unexpected behavior. 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 this chapter.

This section describes caveats in Cisco IOS XE 3.2S releases.

In this section, the following information is provided for each caveat:

- **Symptom**—A description of what is observed when the caveat occurs.
- **Conditions**—The conditions under which the caveat has been known to occur.
- **Workaround**—Solutions, if available, to counteract the caveat.

---

**Note**
If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)
Caveats in Cisco IOS XE 3.2S Releases

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

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

This section consists of the following subsections:

- Open Caveats—Cisco IOS XE Release 3.2.2S, page 364
- Resolved Caveats—Cisco IOS XE Release 3.2.2S, page 364
- Open Caveats—Cisco IOS XE Release 3.2.1S, page 373
- Resolved Caveats—Cisco IOS XE Release 3.2.1S, page 374
- Open Caveats—Cisco IOS XE Release 3.2.0S, page 392

Open Caveats—Cisco IOS XE Release 3.2.2S

This section documents unexpected behavior that might be seen in Cisco IOS XE Release 3.2.2S.

- CSCto32753
  Symptom: When the CES was reloaded or the clear crypto session command was run on the CES, existing IPSec SAs might not be automatically removed.
  Conditions: This issue was observed after the CES was reloaded or the clear crypto session command was run on the CES.
  Workaround: There is no workaround.

- CSCto52235
  Symptom: The mac address accounting command does not work.
  Conditions: There are no specific conditions under which this issue is observed.
  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.2.2S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.2.2S.

- CSCtn71898 and CSCto89992
  Symptom: During an ISSU subpackage upgrade from Release 3.2.x to Release 3.3.0, the router crashes. During an ISSU subpackage downgrade from Release 3.3.0 to Release 3.2.x, the standby RP does not come up correctly after the procedure. Instead, the standby RP reloads continuously and IPC timeout messages are generated each time the RP reloads.
  Conditions: These issues are observed when subpackage ISSU upgrade is performed on the router.
  Workaround: There is no workaround.

- CSCto81063
  Symptom: The IPv6 IPSec SVTI configuration does not work. The router reloads when you try to perform the configuration procedure.
  Conditions: This issue is observed when you try to configure IPv6 IPSec SVTI.
  Workaround: There is no workaround.

- CSCsi18054
Symptom: A local user created with a one-time keyword is automatically removed after failed login attempts. The expected behavior is that the one-time user should be removed after the first successful login, not after failed login attempts.

Conditions: This issue is observed on a router running Cisco IOS Release 12.4.

Workaround: There is no workaround.

- CSCta62394

Symptom: The router reloads automatically when the standby RP tears down all IPSEC SAs.

Conditions: This issue is observed on a router that is running SXF16 with IPSec High Availability and dynamic crypto maps configured on it.

Workaround: Use static crypto maps instead of dynamic crypto maps.

- CSCth52252

Symptom: If multiple EzVPN clients that are behind the same NAT device try to initiate sessions to the dVTI EzVPN server, when the first client connects to the server, traffic passes through the first client. However, when a second client connects to the server, traffic passes through the second client but fails on the first client.

Conditions: This issue is observed when multiple EzVPN clients that are behind the same NAT device try to initiate sessions to the dVTI EzVPN server.

Workaround: There is no workaround.

- CSCtj05903

Symptom: When the router is reloaded, some virtual access interfaces are not created for the VT.

Conditions: This issue is observed on scaled sessions.

Workaround: There is no workaround.

- CSCtj20776

Symptom: During authentication through CoA account login or TAL, a user profile with per-user configuration (such as idle-timeout, accounting, or QoS) is applied to the session. However, after all the actions have been performed, the per-user configuration is not installed and bound to the session.

Conditions: This issue is observed during authentication in which a user profile containing per-user features is downloaded.

Workaround: There is no workaround.

- CSCtj56142

Symptom: In EAP reauthentication-related access requests, the user-name attribute provided may contain a dummy value, which is updated on session by ISG.

Conditions: This issue is observed when EAP access requests carry a dummy user name during EAP reauthentication.

Workaround: There is no workaround.

- CSCtj61748

Symptom: At times, service activation fails.

Conditions: This issue is observed when multiple services in the session authentication or authorization response are configured in the same service group.

Workaround: Remove fields related to service-group and service-type from the service definitions.

- CSCtj79769
Symptom: The router crashes.
Conditions: This issue is observed when either IPv6 MLD snooping is disabled or IPv6 multicast itself is disabled.
Workaround: There is no workaround.

- CSCtj85333

Symptom: The router may crash when the configuration template contains the `ip ips signature-category` configuration command and when the template is downloaded to the router by using the `cns config retrieve` command and the `cns config initial` command.

Conditions: This issue is observed when the configuration commands mentioned in the Symptom description are used. This issue may also occur when the configuration template is downloaded to the router using the Config-Update operation of the configuration engine.

Workaround: There is no workaround.

- CSCtj87846

Symptom: The PfR traffic class does not come out of the default state.
Conditions: This issue is observed when a subinterface is used as an external interface and the corresponding physical interface shuts down and then restarts. The PfR master is not notified that the subinterface has restarted.

Workaround: Shut down and then restart the PfR master or the PfR border.

- CSCtj94510

Symptom: The router crashes at crypto_SS_process.
Conditions: This issue is observed when all of the following conditions exist at the same time:
- DMVPN is configured with more than 1000 tunnels.
- There is one IKE session for each VRF.
- There are four dual SAs per session.

Workaround: There is no workaround.

- CSCtj99431

Symptom: In a session, a shared key mismatch occurs between the ISG and the RADIUS client. However, the nonsubnet client (best match client) gets preference over the subnet client.
Conditions: This issue is observed on a router that is used as an ISG RADIUS proxy router.

Workaround: Remove the `ignore server key` setting from the `aaa server radius dynamic-author` configuration.

- CSCtk18607

Symptom: The router crashes.
Conditions: This issue is observed when `ip ssh pubkey` command is configured in both the user submode and the server submode.

Workaround: There is no workaround.

- CSCtk31401

Symptom: The router crashes when an SSH session is closed.
Conditions: This issue is observed when `aaa authentication banner` command is configured on the router.

Workaround: There is no workaround.
- CSCtk35953
  Symptom: Dampening information is not removed even when dampening is unconfigured in VPNv4 AF.
  Conditions: This issue is observed only if DUT has a eBGP-VPNv4 session with a peer and a same-RD import occurs on the DUT for the route learned from a VPNv4 peer.
  Workaround: Perform a hard reset of the session.

- CSCtk36582
  Symptom: Accounting On and Accounting Off messages from the AZR clear all the sessions in the client pool.
  Conditions: This issue is observed in any of the following scenarios:
  - When there are two AZRs, for example, 192.168.100.1 and 192.168.100.2, and you configure the client in the ISG under the RADIUS proxy as follows:
    `client 192.168.0.0 255.255.0.0`
  - The Accounting On or Accounting Off message from any of the clients clears sessions from both clients.
  Workaround: Configure the clients individually instead of configuring the client pool.

- CSCtk61069
  Symptom: The router crashes.
  Conditions: This issue is observed if you run the `priv exec level level show adjacency` command.
  Workaround: Do not set the privilege exec level for any form of the `show adjacency` command.

- CSCtk62950
  Symptom: Configuring SSH over IPv6 may cause the router to crash.
  Conditions: This issue is observed when SSH over IPv6 is configured.
  Workaround: There is no workaround.

- CSCtk67768
  Symptom: The RP crashes during the DHCPD receive process.
  Conditions: This issue is observed on a DHCP server that is used on a router acting as the ISG.
  Workaround: There is no workaround.

- CSCtk68109
  Symptom: The router reloads automatically when the CVP survivability.tcl script is run.
  Conditions: This issue is observed when `pass-thru content sdp` is used while configuring the router.
  Workaround: Use `codec transparent` instead of `pass-thru content sdp`.

- CSCtk74970
  Symptom: A tunnel that is announced by the TE autoroute is not installed in the routing table.
  Conditions: This issue is observed when you first configure and remove one hop and LDP from the TE, and then configure one hop on the TE (without LDP).
  Workaround: Run the `no ip routing protocol purge interface` command.

- CSCtl00770
  Symptom: The router stops responding during bootup.
  Conditions: This issue is observed when the following secure server WebUI configuration is used:
Caveats in Cisco IOS XE 3.2S Releases

ip http secure-server
!
transport-map type persistent webui map-name secure-server
!
transport type persistent webui input map-name

Workaround: There is no workaround.

- CSCtl04285
Symptom: After provisioning a new BGP session, a BGP route reflector may not advertise IPv4 MDT routes to PEs.
Conditions: This issue is observed on a router running BGP, configured with a new-style IPv4 MDT, and peering with an old-style IPv4 MDT peer.
Workarounds: There is no workaround.

- CSCtl05684
Symptom: XAUTH user information is displayed in the output of the `show crypto session summary` command.
Conditions: This issue is observed when running EzVPN and, at the same time, performing XAUTH using a username that is different from the one used during P1 rekey.
Workarounds: To avoid sending a different username and password during P1 rekey, use the Save Password feature without enabling the interactive XAUTH mode.

- CSCtl21884
Symptom: When enabling autosummary under the BGP process, a BGP withdraw update is not sent even when the static route goes down.
Conditions: This issue is observed under any of the following conditions:
  - Autosummary is enabled under the BGP process.
  - A static route is brought into the BGP table by running the `network` command.
Workarounds: Use the `clear ip bgp *` command. Alternatively, disable the autosummary option under the BGP process.

- CSCtl50815
Symptom: Prefixes remain uncontrolled. In addition, the following message is logged frequently without any actual routing changes:

```
%OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason Non-OER, OOP Reason <reason>
```

Conditions: This issue is observed under the following conditions:
  - ECMP is used.
  - Mode monitor passive is configured.
Workarounds: Remove equal cost routing. For example, in a situation in which you use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one for each exit. This achieves initial load balancing. PfR balances the load correctly as required.

- CSCtl54033
Symptom: After the sub-LSP is pruned or torn down, resignaling sub-LSPs for P2MP TE tunnels may take up to 10 seconds.

Conditions: This issue is observed when a P2MP TE tunnel is configured to request FRR protection, but for the physical link down the path on the tunnel headend, there is no backup tunnel configured at the failure point (TE tunnel headend) to protect the sub-LSP. The TE tunnel headend takes up to 10 seconds to resignal the sub-LSPs.

Workaround: Configure FRR backup tunnels at the TE tunnel headend to provide link protection for P2MP TE tunnels for the physical link that is connected to the TE tunnel headend in the TE tunnel path.

- CSCtl54415
  Symptom: The router may reload.
  Conditions: This issue is observed when single-connection timeout is configured under an AAA group server and a TACACS key is not configured. For example:
  ```
  aaa group server tacacs name server-private x.x.x.x single-connection timeout 2 server-private x.x.x.x single-connection timeout 2 ip tacacs source-interface Loopback0
  ```
  Workaround: Ensure that you configure the correct matching key.

- CSCtl58005
  Symptom: When one of the following commands is run, an accounting start record is sent before an NCP has been negotiated:
  - `aaa accounting include auth-profile framed-ip-address`
  - `aaa accounting include auth-profile delegated-ipv6-prefix`
  - `aaa accounting include auth-profile framed-ipv6-prefix`
  Conditions: This issue is observed when `aaa accounting delay-start` is configured along with one of the commands listed in the Symptom description.
  Workaround: There is no workaround. If possible, avoid using the commands listed in the Symptom description.

- CSCtl67195
  Symptom: The following BGP debug commands do not run correctly:
  - `debug ip bgp vpnv4 unicast`
  - `debug ip bgp vpnv6 unicast`
  - `debug ip bgp ipv6 unicast`
  Conditions: This issue is observed when the BGP debug commands mentioned in the Symptom description are run.
  Workaround: There is no workaround.

- CSCtl83736
  Symptom: A V4 session setup leaks approximately 100 bytes. The following command can be used to verify the existence of this issue:
  ```
  show platform software memory messaging ios rp active | inc st_sb_cfg
  ```
  In the output of this command, the `diff` number increases continuously.
  Conditions: This issue is observed in IP sessions.
  Workaround: There is no workaround.
- **CSCtl84797**
  Symptom: SBC traceback occurs.
  Conditions: This issue is observed when LI is enabled and there are multiple media sessions in a single call (that is, SDP contains information about multiple media sessions).
  Workaround: There is no workaround.

- **CSCtl88066**
  Symptom: The router reloads automatically.
  Conditions: This issue is observed when BGP is configured and one of the following commands is run:
  - `show ip bgp all attr nexthop`
  - `show ip bgp all attr nexthop rib-filter`
  Workaround: Do not run either of these commands with the `all` keyword. Instead, run the address-family-specific version of the command for the address family.

- **CSCtn01832**
  Symptom: The following sequence of commands causes the router to crash at check syntax mode:
  1. `config check syntax route-map hello`
  2. `match local-preference`
  3. `no match local-preference`
  Conditions: This issue is observed when the sequence of commands mentioned in the Symptom description is run.
  Workaround: There is no workaround.

- **CSCtn03930**
  Symptom: System error messages are recorded in the router log.
  Conditions: This issue is observed on a router that functions as an IPSec termination and aggregation router. The issue occurs when RP switchover takes place while traffic is being processed.
  Workaround: There is no workaround.

- **CSCtn07415**
  Symptom: The router crashes at `crypto_map_get_map_method_bitmask`.
  Conditions: This issue is observed while reconfiguring IPSec with a large number (for example, 1300) of GRE tunnel interfaces while old configurations are present.
  Workaround: There is no workaround.

- **CSCtn18784**
  Symptom: Interface tunnel 0 sends constant high-bandwidth alarms.
  Conditions: There are no specific conditions under which this issue is observed.
  Workaround: There is no workaround.

- **CSCtn22728**
  Symptom: When running the `exi exi` command in the EVC mode, the standby RP may reload automatically due to configuration mismatch.
  Conditions: This issue is observed when the `exi exi` is run in the EVC mode.
  Workaround: There is no workaround.
• CSCtn24024
Symptom: A router on which dynamic crypto maps are configured may experience a condition in which an IPSec SA decrypts traffic but does not encrypt traffic.
Conditions: In general, this issue is observed when the remote peer IP address has changed. A duplicate flow is created in the hardware and, therefore, the traffic to be encrypted matches a stale flow.
Workaround: Clearing the crypto session from the spoke might resolve the issue.

• CSCtn25100
Symptom: PPP sessions take longer to start.
Conditions: There are no specific conditions under which this issue is observed.
Workaround: There is no workaround.

• CSCtn42916
Symptom: In a redundant RP setup, when the active RP is physically removed from the chassis, the standby RP crashes.
Conditions: This issue is observed on routers on which ASR1000-ESP40 is installed.
Workaround: There is no workaround for this issue. Where possible, instead of performing a hardware OIR, perform an OIR by using the CLI.

• CSCtn53094
Symptom: The router crashes or generates the following error message:

%SYS-3-MGDTIMER: Timer has parent, timer link, timer = 8796350. -Process= "Mwheel Process", ipl= 2, pid= 315

Conditions: This issue is observed when alternating, with a very small delay, between the `ip pim mode` and `no ip pim` commands on an interface that is the only one on which PIM is enabled. The most common way this occurs in a production network is with the use of the `config replace` command, which results in the command alternating between ON and OFF and then to ON on a different interface.
Workaround: There is no workaround. Avoid alternating between the `ip pim mode` and `no ip pim` commands on an interface that is the only one on which PIM is enabled.

• CSCtn56526
Symptom: MBS is calculated on the basis of the MTU value. The user-defined MBS value is not displayed when the `sh atm pvc` command is run.
Conditions: This issue is observed when a user-defined MBS value is set using the CLI.
Workaround: There is no workaround.

• CSCtn59698
Symptom: When an MLP bundle comes up on an LNS with conditional debugging based on the username that is enabled, certain attributes such as IDB description and IP-VRF are not applied on the MLP bundle virtual access interface.
Conditions: This issue is observed when all the following conditions exist at the same time:
- MLP sessions are configured on the LNS.
- Per-user attributes, such as ip:vrf-id and ip:description, are configured in the user's RADIUS profile.
- The session is started.
- The show interfaces Virtual-Access_intf configuration command is run for both the member-link VA and the bundle VA.
- The VRF and IDB descriptions sent by the RADIUS server is applied only on the member-link VA and not on the bundle VA.

Workaround: Do not enable conditional debugs such as debug condition username username.

- CSCtn60353
  Symptom: When subpackage ISSU is performed, some OM objects on the standby RP may be missing.
  Conditions: This issue is observed when ISSU is performed across two releases and the target release adds a new TDL message type.
  Workaround: Force a reload of the standby RP before the final RP switchover.

- CSCtn64500
  Symptom: Multicast traffic does not pass through an ATM point to a multipoint sub-interface.
  Conditions: This issue is caused by an incomplete inject p2mp multicast adjacency on ATM P2MP interface. The output of the show adjacency ATM interface detail command shows that the Inject p2mp Multicast adjacency is in incomplete state.
  Workaround: Run the clear adjacency command to force repopulate the incomplete adjacency. Note that you should be aware of the impact of this system-wide command. As an alternative, use unicast commutation if it is possible to do so.

- CSCtn70367
  Symptom: The IPSec key engine crashes while sessions are being set up.
  Conditions: This issue is observed while setting up sessions with the configuration of 1000 VRFs, 1 IKE session per VRF, and 4 IPSec SA dual per session. The crash occurs while UUT is establishing the requested SAs.
  Workaround: There is no workaround.

- CSCtn73941
  Symptom: After performing an OIR for an ES+ card having EVC configuration with the module clear-config command enabled, reapplying the previous configuration does not work. In other words, traffic is not forwarded over the service instances. Even after changing the service instance numbers, the VLANs used in the previous configuration cannot be used effectively on the ports.
  Conditions: This issue is observed when module clear-config is configured.
  Workaround: There is no workaround.

- CSCtn81231
  Symptom: Multicast traffic is not forwarded from the RBE interface because the multicast adjacency is incomplete.
  Conditions: This issue is observed when the ATM DCHP host running IGMPv2 is established over an RBE interface to the router. The multicast group join is successful. However, the multicast adjacency is incomplete and it cannot forward multicast traffic.
  Workaround: Shut down and then restart the ATM main interface.
• CSCto03123
   Symptoms:
   1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
   2. Additional memory leak can occur when frequent sensor value changes take place.
   Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.
   Workaround: There is no workaround.
   PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.
   If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.
   Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

• CSCto08790
   Symptom: When BRAS applies an ANCP shaper with a specific policy map name, ActualDownstreamRate, and dslType value, a policy map is created with a policy map name resulting in hash value 0. Because a policy map name with a hash value 0 is not handled properly by the QoS client, the router crashes.
   Conditions: This issue is observed when BRAS applies an ANCP shaper with a specific policy map name, ActualDownstreamRate, and dslType value.
   Workaround: There is no workaround.

• CSCto40479 and CSCto89992
   Symptom: During an ISSU subpackage upgrade from Release 3.2.x to Release 3.3.0, the router crashes. During an ISSU subpackage downgrade from Release 3.3.0 to Release 3.2.x, the standby RP does not come up correctly after the procedure. Instead, the standby RP reloads continuously and IPC timeout messages are generated each time the RP reloads.
   Conditions: This issue is observed when subpackage ISSU is performed on the router.
   Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.2.1S

This section documents unexpected behavior that might be seen in Cisco IOS XE Release 3.2.1S.

• CSCtl71478
   Symptom: In an HA system, the following error message is displayed on the standby RP and LC:
   OCE-DFC4-3-GENERAL: MPLS lookup unexpected
   Conditions: This issue is observed when both the RP and the standby/LC routers are brought up either with or without configuration.
   Workaround: There is no workaround.

• CSCta37670
Symptom: The router crashes when the watchdog times out.
Conditions: This issue is observed on adding a large number of routes in IXIA, which causes an increase in the size of the IP VRF table.
Workaround: There is no workaround.

- CSCt67150
  Symptom: Multilink interfaces take more than 30 seconds to start up.
  Conditions: This issue is observed with all multilink interfaces.
  Workaround: There is no workaround. Note that the delay in starting up does not affect the working of the multilink interfaces.

- CSCto03123
  Symptoms:
  1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
  2. Additional memory leak can occur when frequent sensor value changes take place.
  Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.
  Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

### Resolved Caveats—Cisco IOS XE Release 3.2.1S

This section documents issues that have been resolved in Cisco IOS XE Release 3.2.1S.

- CSCta43825
  Symptom: A CMTS or SNMP walk of the ARP table causes high CPU usage.
  Conditions: This issue is observed when a CMTS or SNMP walk of the ARP table is performed.
  Workaround: To prevent an SNMP walk of the ARP table, implement an SNMP view by using the following commands:

```
snmp-server view cutdown iso included
snmp-server view cutdown at excluded
snmp-server view cutdown ip.21 excluded
snmp-server community public view cutdown ro
snmp-server community private view cutdown rw
```

- CSCtd72318
  Symptom: The Cisco ASR 1004 Router crashes at in_be_dhcpc_for_us.
Conditions: This issue is observed in Cisco IOS Release 12.2(33)XNC2. It may be associated with the DHCP configuration.
Workaround: There is no workaround.

- CSCtd94789
Symptom: The IPSEC rekey fails after failover when stateful IPSEC HA is in use.
Conditions: This issue is observed when using PFS, after a failover of the hub devices.
Workaround: If the security policy permits it, then remove the PFS.

- CSCte65688
Symptom: When the software VPN client establishes an IPsec session, the EzVPN server prints the following message:

```
Client_type=UNKNOWN message in the %CRYPTO-6-EZVPN_CONNECTION_UP: (Server) log
```

Conditions: This issue is observed when EzVPN is configured between a Cisco VPN client and router and crypto logging ezvpn is configured.
Workaround: There is no workaround.

- CSCtf41721
Symptom: A DMVPNv6 hub might crash when the tunnel interface of the other hub is shut down and then restarted.
Conditions: This issue is observed if DMVPNv6 is configured with two hubs and two spokes, and a certain set of commands are run in a specific sequence.
Workaround: There is no workaround.

- CSCtf81621
Symptom: Line-By-Line configuration synchronization fails, and the standby RP is reloaded.
Conditions: This issue is observed while configuring protocol ppp virtual-template under the ATM PVC mode.
Workaround: Configure no policy config-sync lbl prc reload.

- CSCth03022
Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.
Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

- CSCti36310
Symptom: The router might leak memory when IKE attributes are pulled by SNMP.
Conditions: This issue is observed on a router on which SNMP is enabled.
Workaround: There is no workaround.

- CSCti47252
Symptom: SBC can attach an adjacency even when a wrong remote address is configured for the redundant peer.
Conditions: This issue is observed when a wrong remote address is configured for the redundant peer.
Workaround: There is no workaround.

- CSCti48504
  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.
  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

- CSCti54173
  Symptom: A leak of 164 bytes of memory for every packet that is fragmented at high CPU is seen after all the processor memory is leaked. This causes the router to reload.
  Conditions: This issue is observed after all the processor memory is leaked.
  Workaround: There is no workaround.

- CSCti66454
  Symptom: The router crashes when the `show crypto session detail` command is run after the `clear crypto session` command is run.
  Conditions: This issue is observed if the `clear crypto session` command is run while the router is running some form of tunnel protection.
  Workaround: After running the `clear crypto session` command, wait for at least 30 seconds before running the `show crypto session detail` command.

- CSCti94938
  Symptom: The router crashes when a nonexistent route map is applied and then modified.
  Conditions: This issue is observed when there is more than one L2TP session on the virtual template interface.
  Workaround: Configure the route map before applying the policy.

- CSCti98931
  Symptom: Some sessions may be lost after an L2TP switchover.
  Conditions: This issue is observed after an L2TP switchover.
  Workaround: There is no workaround.

- CSCtj14525
  Symptom: After a new policy is attached, the standby RP is not switched to active state in the event that the active RP crashes.
  Conditions: This issue is observed after a new policy is attached.
  Workaround: There is no workaround.
- **CSCtj29831**
  
  **Symptom:** The router crashes after an SSO.
  
  **Conditions:** This issue is observed when an IPv6 named and tagged ACL is applied through the service logon.
  
  **Workaround:** There is no workaround.

- **CSCtj40564**
  
  **Symptom:** The router does not allow an incoming IKE connection even if the keyring is matched.
  
  **Conditions:** This issue is observed after the router is reloaded and when a crypto keyring having a local address defined as an interface is used.
  
  **Workaround:** Use an IP address.

- **CSCtj51139**
  
  **Symptom:** ASR1000-SIP40 crashes due to a low-memory condition.
  
  **Conditions:** This issue is observed when a large number of PPPoA sessions are started on a single SIP40 with autovc and autosense configured.
  
  **Workaround:** Apply one of the following workarounds:
  
  - Reduce the number of sessions on a single SIP40 (14000 or fewer).
  - Enable either autovc or autosense (not both) at any point of time to reduce the number of IPC messages.

- **CSCtj73848**
  
  **Symptom:** The bba_ipv6_lns traffic fails after an RP switchover.
  
  **Conditions:** This issue is observed after an RP switchover.
  
  **Workaround:** There is no workaround.

- **CSCtj77004**
  
  **Symptom:** The size of the archive log configuration impacts CPU usage during PPPoE establishment. In addition, only some configuration lines from the virtual template are copied to the archive. The remaining lines are not copied.
  
  **Conditions:** This issue is observed when `archive log config` is configured.
  
  **Workaround:** There is no workaround.

- **CSCtj82401**
  
  **Symptom:** After the router is rebooted, all adjacencies get detached and all calls fail.
  
  **Conditions:** If the configured default call policy contains `na-carrier-id-table`, it is converted to `na-dst-carrier-id-table`. During reboot, `na-dst-carrier-id-table` is detected as an unrecognized command and that part of the configuration is rejected. This leaves SBC in a state where all adjacencies are detached until the problem is corrected.
  
  **Workaround:** Manually add `na-carrier-id-table` back to the configuration after reloading the router. After adding `na-carrier-id-table`, deactivate and then reactivate SBC.

- **CSCtj82405**
  
  **Symptom:** After a chassis is reloaded, the secondary IP address configured on the SBC interface is automatically removed. Because this is the media address, all subsequent calls fail because there is no functional media address.
  
  **Conditions:** This issue is observed after a chassis is reloaded.
Caveats in Cisco IOS XE 3.2S Releases

- CSCtj89941
  Symptom: IOS crashes when the clear crypto session command is used on an EzVPN client.
  Conditions: This issue is observed when the clear crypto session command is used on an EzVPN client.
  Workaround: There is no workaround.

- CSCtj94490
  Symptom: The RP reloads after 30 RP switchovers.
  Conditions: This issue is observed when a large number of PPoEoA sessions are present and when traffic is flowing.
  Workaround: There is no workaround.

- CSCtj99466
  Symptom: The volume-based SA lifetime is set to 0 on almost all the sessions while bringing up a large number of SVTI tunnels on a router with RP1. This results in traffic not getting encrypted and decrypted on those tunnels.
  Conditions: This issue is observed after performing a sequence of steps that clear all crypto sessions.
  Workaround: There is no workaround.

- CSCtk00398
  Symptom: On receiving DHCPv6 SOLICIT from two clients with the same DUID, DHCPV6 binds the delegated prefix to the wrong client.
  Conditions: This issue is observed when two clients send SOLICIT messages with the same DUID.
  Workaround: There is no workaround.

- CSCtk06750
  Symptom: IP-directed broadcast packets do not get forwarded by a downstream router.
  Conditions: When link encapsulation is set to HDLC, layer frames are sent out with an incorrect address type. Therefore, the downstream router does not forward them further as directed broadcast packets.
  Workaround: Change the encapsulation to PPP on the affected serial interfaces.

- CSCtk12252
  Symptom: A Priority 1, valid SONET controller network clock source is not selected as the active clock source. Instead, the clock remains in the FREERUN state.
  Conditions: This issue is observed after the router is reloaded, and when a valid, but absent, Priority 2 network clock source is specified.
  Workaround: Shut down and then restart the near-end Priority 1 clock source SONET controller.

- CSCtk12708
  Symptom: The router crashes when the holdover clock source is deleted.
  Conditions: This issue is observed when the holdover clock source is deleted.
  Workaround: There is no workaround.

- CSCtk30508
Symptom: After a FRoMPLS PW is torn down, the connect object stays in FMAN-RP, FMAN-FP, and CPP. This causes memory leakage. It may also cause failure in creating a FRoMPLS PW.
Conditions: There are no specific conditions under which this issue is observed.
Workaround: There is no workaround.

- CSCtk30807
  Symptom: A router that acts as a DHCP relay server crashes when the DHCP service is shut down by first running the `no service dhcp` command and then restarted by running the `service dhcp` command.
  Conditions: This issue is observed when the router is also configured as the ISG.
  Workaround: There is no workaround.

- CSCtk34287
  Symptom: MFIB does not delay release of MDT adjacency when capability is configured.
  Conditions: This issue is observed when capability is configured.
  Workaround: There is no workaround.

- CSCtk35599
  Symptom: During a slow-start to slow-start H.323 call, the initial bandwidth that is requested is the same as that required for a voice call. This might cause video call degradation when interworking with VCS-E.
  Conditions: This issue is observed when interworking with VCS-E.
  Workaround: There is no workaround.

- CSCtk54431
  Symptom: When a router BRAS receives SOLICIT IA-PD from the CPE, but no Delegated-IPv6-Prefix is received from RADIUS, no reply is sent to the CPE. The expected response is that an Advertise with the NoPrefixAvail option is sent.
  Conditions: This issue is observed when the CPE requests IA-PD, but BRAS does not have a Delegated-IPv6-Prefix.
  Workaround: There is no workaround.

- CSCtk67176
  Symptom: When billing is configured, the CDR media-info CLI is not automatically enabled.
  Conditions: This issue is observed when billing is configured.
  Workaround: There is no workaround.

- CSCtk68647
  Symptom: DMVPN disallows connections after a certain number of connections are established. The `show crypto socket` command shows that sockets are leaking and do not stop even when the SA is inactive.
  Conditions: This issue is observed in releases earlier than Cisco IOS Release XE 3.2.0 and when multiple DMVPN tunnels are configured with tunnel protection shared.
  Workaround: Upgrade to Cisco IOS Release XE 3.2.0, and remove or shut down the other DMVPN tunnels.

- CSCtk75389
  Symptom: The PfR fallback interface does not remain in policy.
Caveats in Cisco IOS XE 3.2S Releases

Conditions: This issue is observed on the ATM interface.
Workaropus: There is no workaround.

- CSCtl00127
  Symptom: The output of the `show ip int` command does not indicate whether the `ip security ignore-cipso` option is configured and operational.
  Conditions: There are no specific conditions under which this issue is observed.
  Workaropus: There is no workaround.

- CSCtl05979
  Symptom: In SSO mode, PPPoE sessions with PAC2 ISG service are replicated on the standby RP, with policy maps missing on the standby RP. The expected behavior is that the PAC2 service must poison the PPPoE sessions.
  Conditions: This symptom is observed in SSO mode, when PPPoE sessions with the PAC2 ISG service are established.
  Workaropus: Use the dummy ISG service applied from RaBaPol to force poisoning.

- CSCtl08014
  Symptom: The router crashes with memory corruption symptoms.
  Conditions: This issue is observed when performing switchover or OIR when MLP sessions are getting initiated.
  Workaropus: There is no workaround.

- CSCtl20993
  Symptom: The router crashes during IPsec rekey.
  Conditions: There are no specific conditions under which this issue is observed.
  Workaropus: There is no workaround.

- CSCtl49769
  Symptom: SBC does not report the media address in a Lawful Intercept IRI message. In a Lawful Intercept environment, the expected behavior is that the media IP address and port details of the parties in the call must be reported to the MF so that the Call Content-tapped traffic can identify the direction of the media flow.
  Conditions: This issue is observed during normal call flow.
  Workaropus: There is no workaround.

- CSCtl50930
  Symptom: For some SIP messages (for example, OPTION), SBC asserts failure when the call is sent through VRF.
  Conditions: This issue is observed on the Cisco ASR 1001, 1002, and 1004 Routers in nonredundant mode.
  Workaropus: Configure redundant mode SSO.

- CSCtl83053
  Symptom: The Shaper rate cannot be changed by using ANCP Port Up messages.
  Conditions: This issue is observed on a router with QOS and ANCP enabled.
  Workaropus: There is no workaround.
Caveats in Cisco IOS XE 3.2S Releases

- **CSCtl42358**
  Symptom: The router crashes after the `no atm sonet overhead j1` message is issued.
  Conditions: There are no specific conditions under which this issue is observed.
  Workaround: There is no workaround.

- **CSCtl74301**
  Symptom: INBOX SSO does not work on the Cisco ASR 1006 Router. When this occurs, SSO drops signaling and RTP.
  Conditions: This issue is observed during INBOX SSO. This occurs when SIP binds with the loopback address for control.
  Workaround: There is no workaround. Unless required by your network architecture, do not use a loopback address for control bind.

- **CSCtd16959**
  Symptom: Traceback is seen on SSO switchover.
  Conditions: This issue is observed when the following steps are performed:
  - The CBTS master tunnel is configured with three member tunnels.
  - The member tunnels are deleted and then the master command is removed from the master tunnel so that it becomes a regular TE tunnel.
  - The auto-tunnel primary and backup setup are configured.
  - SSO switchover is performed.
  Multiple tracebacks are seen on the newly active RP, which are related to MPLS TE.
  Workaround: Do not delete the CBTS tunnels.

- **CSCte51529**
  Symptom: CUBE does not forward 491 Request Pending responses.
  Conditions: This issue may be observed during a consultative call transfer flow.
  Workaround: There is no workaround.

- **CSCtf23298**
  Symptom: There is high CPU usage when a TACACS server is configured with a single connection.
  Conditions: This issue is observed when a TACACS server is configured with a single connection.
  Workaround: Remove the single connection option.

- **CSCtf72328**
  Symptom: The BFD IPv4 Static feature does not fully support the Administratively Down status.
  Conditions: This issue is observed because the BFD APIs do not notify its clients about the Administratively Down status. If the clients do not receive notification about the BFD peer Administratively Down status, then they consider the BFD peer to be up and running.
  Workaround: Shut down and then restart the interface on which the BFD session is configured.

- **CSCtg28806**
  Symptom: The router crashes during PKI manual enroll.
  Conditions: This issue is observed on a router running Cisco IOS Release 15.0(1)M1.
  Workaround: There is no workaround.
- **CSCtg64175**
  Symptom: The IS-IS route is missing the P2P link. It is incorrectly marked as parallel p2p adjacency suppressed.
  Conditions: This issue is observed when the IS-IS neighbor is up and multiple topologies are enabled on P2P interfaces. It is observed when you enable a topology on a P2P interface of the remote router and send out the serial IIH packet with the new MTID to the local router where the topology has not yet been enabled on the local P2P interface.
  Workaround: Shut down and then restart the local P2P interface.

- **CSCth13415**
  Symptom: One-way audio in call transfer due to 491 response during resume re-INV.
  Conditions: This issue is observed when there is an UPDATE message passing through the CUBE and then a re-INV crossover occurs. The re-INV crossover results in a 491, but the 491 is not correctly forwarded by the IPIP GW. This may result in one-way audio if the crossed-over re-INV was in the process of changing the state of the media from Hold to Resume.
  Workaround: There is no workaround.

- **CSCth37580**
  Symptom: The dampening route is present even after removing BDP dampening.
  Conditions: This issue is observed under the following conditions:
  - DUT connects to RTRA with eBGP VPNv4.
  - eBGP VPNv4 peer session is established and DUT.
  - DUT has VRF (same RD) as the route advertised by RTRA. In this scenario, when DUT learns the route it performs the same RD import. In addition, the topology of the net is changed from VPNv4 to VRF.
  Workaround: There is no workaround.

- **CSCth61759**
  Symptom: Video call fails with CVTA.
  Conditions: This issue is observed when there is an end-to-end SIP flow around the call with CVTA.
  Workaround: There is no workaround.

- **CSCth93218**
  Symptom: The %OER_BR-4-WARNING: No sequence available error message is displayed on PfR BR.
  Conditions: This issue is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.
  Workaround: There is no workaround.

- **CSCti08811**
  Symptom: The router may reload when running commands through an Embedded Event Manager (EEM) policy.
  Conditions: This issue is observed only when EEM policies are used.
  Workaround: There is no workaround.

- **CSCti22091**
Symptom: Traceback occurs after the **show oer master** command is used a few times. The traceback is always followed by the **learning writing data** message. The traceback causes the OER system to be automatically disabled. Manually re-enabling PfR does not work, and a reboot is required.

Conditions: This issue is observed when the following procedure is performed:

3. In the list submode of PfR, a traffic-class application is configured with a prefix list as the filter.
4. In the traffic-class submode of PfR, keys are configured and then an ACL is configured as a filter.

Workaround: There is no workaround.

- **CSCti25319**

Symptom: A directly connected subnet that is covered by a network statement is not redistributed into another routing protocol, even if a redistribute OSPF is configured.

Conditions: This issue is observed only on configurations in which a network mask covers multiple supernets.

Workaround: Apply one of the following workarounds:

- Enable OSPF using the **ip ospf AS area** interface command.
- Configure multiple network statements with the mask/wildcard equal to the supernet as shown in the following example:
  
  ```
  router ospf 1 network 192.168.0.0 0.0.0.255 area 0 network 192.168.1.0 0.0.0.255 area 0
  ```

- **CSCti34396**

Symptom: The router distributes an unreachable next-hop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

Conditions: This issue is observed when **next-hop-unchanged allpaths** is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is unreachable.

Workaround: Apply one of the following workarounds:

- Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside it.
- Instead of configuring static routes with a next-hop, specify an interface name.

- **CSCti51145**

Symptom: After a reload of one router, some or all of the BGP address families do not become active. The output of the **show ip bgp all summary** command shows the address family in NoNeg or Idle state, and it remains in that state.

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

- The non-reloading device has a **neighbor x.x.x.x transport connection-mode passive** configuration. Alternatively, there is an IP ACL or packet filter that permits connections initiated by the reloading device, but not by the non-reloading device.
- The BGP hold time that is configured is less than the time required for neighbor x.x.x.x to reload.
- When neighbor x.x.x.x reloads, no keepalives or updates are sent on the stale session during the interval between the time the interface comes up and neighbor x.x.x.x exchanges BGP open messages.
- Both peers are multisession capable.
- The **transport multi-session** setting is not configured or enabled by default on either device.
- The **graceful restart** setting is not configured.

Workaround: Apply one of the following workarounds:

- Remove the `neighbor x.x.x.x transport connection-mode passive` configuration or edit the corresponding filter or IP ACL to permit the active TCP to open in both directions.
- Configure the `neighbor x.x.x.x transport multi-session` setting on either the device or its neighbor.
- Configure a very short keepalive interval (such as 1 second) on the nonreloading device by using the `neighbor x.x.x.x timers 1 holdtime` command.
- Configure graceful restart by using the `neighbor x.x.x.x ha-mode graceful-restart` command.
- If this issue occurs, use the `clear ip bgp *` command to cause all sessions that are in the NoNeg state to restart. Alternatively, you can use the `clear ip bgp x.x.x.x addressFamily` command to bring up individual sessions without resetting everything.

- **CSCti61949**
  
  Symptom: The router reloads and the SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header and chunk name is BGP (3) update messages are displayed.
  
  Conditions: This issue is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.
  
  Workaround: Disable multicast routing on VRFs participating in BGP. Alternatively, reduce the number of extended communities used as route target export.

- **CSCti67102**
  
  Symptom: A tunnel is automatically disabled due to the creation of a recursive routing loop in RIB.
  
  Conditions: This issue is observed when a dynamic tunnel that is passive by default is created. EIGRP receives a callback due to the address change (dynamic tunnel comes up). EIGRP tries to run on this interface and install an EIGRP route in the RIB, which replaces the tunnel next-hop.
  
  Workaround: There is no workaround.

- **CSCti68721**
  
  Symptom: The output of the `show performance monitor history interval <all | given #>` command shows an extra column.
  
  Conditions: This issue is observed when traffic runs on a performance monitor policy at the time when a user runs the `show` command.
  
  Workaround: Repeat the command when this issue is observed.

- **CSCti81136**
  
  Symptom: Running the `no ip route-cache` command on an interface results in both `no ip route-cache` and `no ip route-cache cef` appearing in the configuration.
  
  Conditions: This issue is observed when the `no ip route-cache` command is run on an interface.
  
  Workaround: There is no workaround.

- **CSCti84762**
  
  Symptom: Update generation does not proceed, and some peers remain in the refresh started state (SE).
  
  Conditions: This issue is observed when there is peer flap, route churn, or interface flap.
  
  Workaround: Hard reset the peers that are in the SE state.

- **CSCti85446**
Symptom: A next-hop static route is not added to RIB even though the next-hop IP address is reachable.

Conditions: This issue is observed after the following sequence of actions and events:
1. A next-hop static route is configured with a permanent keyword.
2. The next-hop IP address becomes unreachable.
3. Change the configuration in such a way that the next-hop is reachable.
4. Configure a new static route through the next-hop IP address used in step 1.

Workaround: Delete all the static routes through the affected next-hop, and then add them again.

- **CSCti91215**
  Symptom: The router stops responding.
  Conditions: This issue is observed while removing the address family a second time.
  Workaround: There is no workaround.

- **CSCti92450**
  Symptom: OSPFv3 graceful restart does not terminate gracefully because it remains in pending state on a loopback interface.
  Conditions: This issue is observed when there is at least one loopback interface with OSPFv3 configured.
  Workaround: There is no workaround.

- **CSCtj05670**
  Symptom: During SSO with scaled mLDP configuration, the path set for some VRFs are not configured.
  Conditions: This issue is observed while configuring mLDP on 100 VRFs with 100 receivers.
  Workaround: There is no workaround.

- **CSCtj08533**
  Symptom: QoS classification fails on the egress PE if the route is learned through BGP.
  Conditions: This issue is observed when there are redundant paths to the CPE.
  Workaround: Use only one path between the PE and CPE.

- **CSCtj11322**
  Symptom: The AAA server is not able to decode RADIUS attributes.
  Conditions: There are no specific conditions under which this issue is observed.
  Workaround: There is no workaround.

- **CSCtj17316**
  Symptom: EIGRP flaps in a large-scale network with a large amount of traffic.
  Conditions: This issue is observed in a large-scale network with a large amount of traffic.
  Workaround: Apply one of the following workarounds:
  - Find the instability in the network, and fix the interface.
  - Summarize the routes.
  - Change more routers to stub.
  - Upgrade to Release 7 of EIGRP.
- CSCtj17545
  Symptom: After a switchover, the restarting speaker sends TCP-FIN to the receiving speaker when the receiving speaker tries to establish a connection. This may cause packets to be dropped after the switchover.
  Conditions: This issue is observed when a large number of BGP peers are established on different interfaces.
  Workaround: Configure the receiving speaker to accept passive connections.

- CSCtj24453
  Symptom: Traceback is observed when the `clear ip bgp *` command is run.
  Conditions: This issue is observed when there are relatively few routes and route-map-cache entries.
  Workaround: Use the `no bgp route-map-cache` command.

- CSCtj28747
  Symptom: Route control of prefix and application are out of order. This makes application control ineffective. The `Exit Mismatch` message is logged, and the application becomes uncontrolled for a short interval before it comes back under control.
  Conditions: This issue is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR.
  Workaround: There is no workaround.

- CSCtj32574
  Symptom: Removal of the `redistribute` configuration in EIGRP is not synchronized to the standby RP.
  Conditions: This issue is observed when any redistribute-related command is run.
  Workaround: There is no workaround.

- CSCtj32769
  Symptom: Data path fails with L2VPN on an ACR interface.
  Conditions: This issue is observed when a VPN is configured on an ACR interface in asynchronous mode with cell-packing configurations. This issue is not observed in normal synchronous mode or L2VCs.
  Workaround: Configure the same MNCP value for local and remote PE devices.

- CSCtj36521
  Symptom: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the `show ip mfib interface` command shows the interface as being configured and available, when it should be disabled.
  Conditions: This issue is observed only if IPv6 CEF is enabled at the same time.
  Workaround: Ensure that IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if you are running a mixed IPv4/IPv6 environment.

- CSCtj38579
  Symptom: FlexWan crashes continuously with Tunnel QoS.
  Conditions: This issue is observed with pim-register ratelimit.
  Workaround: There is no workaround.

- CSCtj45084
Symptom: A crash occurs when the `clear ip ospf process` command is run in a multicast configuration.
Conditions: This issue is observed when the `clear ip ospf process` command is run in a multicast configuration.
Workaround: There is no workaround.

- CSCtj47736
  Symptom: The router crashes when the `show eigrp service ipv4 neighbor` command is run.
  Conditions: This issue is observed when the neighbor is learned, you add a max-service limit on an address family, and you then shut down and restart the interface.
  Workaround: There is no workaround.

- CSCtj48629
  Symptom: Although the `ppp multilink load-threshold 3 either` setting is configured, member links are not added by the inbound heavy traffic on the PRI of the HWIC-1CE1T1-PRI.
  Conditions: There are no specific conditions under which this issue is observed.
  Workaround: There is no workaround.

- CSCtj52564
  Symptom: The router crashes when removing the `pppoe-client` configuration from the VC.
  Conditions: This issue is observed when you try to remove the `pppoe-client` configuration by running the `no pppoe-client` command on the VC.
  Workaround: There is no workaround.

- CSCtj58943
  Symptom: The standby RP reloads due to line-by-line sync failure when the `encapsulation dot1q 1381` command is run.
  Conditions: This issue is observed when a configuration command is run in the subinterface mode.
  Workaround: There is no workaround.

- CSCtj64728
  Symptom: After the VNET tag value is reconfigured, a member switch console cannot be accessed after stack bootup.
  Conditions: This issue is observed after the VNET tag value is reconfigured.
  Workaround: There is no workaround.

- CSCtj64940
  Symptom: When a police rate is set for values more than 4 Gbps (for example, on 10 Gbps Ethernet), the actual rate is incorrectly set to some random value.
  Conditions: This issue is observed only when police rate configurations are more than 4 Gbps.
  Workaround: There is no workaround.

- CSCtj65553
  Symptom: A static route entry created in the default table is automatically deleted.
  Conditions: This issue is observed after a Route Processor to Line Card to Route Processor transition on the Cisco Catalyst 3000 series switching module.
  Workaround: Manually configure the missing static route.
- CSCtj67794
  Symptom: IPv6 multicast RPF lookup fails when the primary static default route is unreachable and replaced by the standby static route.
  Conditions: This issue is observed when two or more IPv6 static routes are configured as the default route with metric. After the primary default route is lost and replaced by the standby static route, multicast RPF fails and multicast traffic is affected.
  Workaround: Configure a static default route with an outgoing interface.

- CSCtj72730
  Symptom: When an EIGRP address-family configuration is removed, a redistribution command that refers to the address-family is not removed. The expected behavior is that all redistribution commands should be removed.
  Conditions: This issue is observed when an EIGRP address-family configuration command is removed.
  Workaround: Manually remove the redistribution commands that are not removed after the address-family command is removed.

- CSCtj74570
  Symptom: The router crashes when trying to check the PVC command syntax in the syntax check mode.
  Conditions: This issue is observed when you try to run the `pvc` command in the syntax check mode without having a PVC created during configuration that is carried out before the syntax check.
  Workaround: There is no workaround.

- CSCtj79750
  Symptom: Multicast responses are not received.
  Conditions: After a Multicast Listener Discovery (MLD) join, multicast responses are not received.
  Workaround: There is no workaround.

- CSCtj82292
  Symptom: EIGRP summary address with AD 255 are sent to the peer.
  Conditions: This issue occurs when a summary address is advertised as shown in the following example:

  ```
  ip summary-address eigrp AS# x.x.x.x y.y.y.y 255
  ```
  Workaround: There is no workaround.

- CSCtj84389
  Symptom: A member switch cannot be accessed after stack bootup.
  Conditions: This issue is observed when IEEE 802.1x is configured.
  Workaround: There is no workaround.

- CSCtj87180
  Symptom: When an LAC router receives an invalid redirect from a peer running VPDN, it may crash with the following CDN error message:

  ```
  SSS Manager Disconnected Session
  ```
  Conditions: This issue is observed when the LAC router receives an incorrect error from the multi-hop peer.
Caveats in Cisco IOS XE 3.2S Releases

Symptom: The router might crash when CEF forwarding is enabled.
Conditions: CEF optimise neighbour resolution must be enabled for the address family (IPv4 or IPv6). A packet destined for an unknown neighbor on an Ethernet interface matches the connected prefix for that Ethernet, and triggers a glean operation.
Workaround: Depending on the address family whose CEF is forwarding, apply one of the following configurations:

```
no ip cef optimize neighbor resolution
no ipv6 cef optimize neighbor resolution
```

Symptom: The LNS router stops responding at interrupt level and enters an infinite loop.
Conditions: There are no specific conditions under which this issue is observed.
Workaround: There is no workaround.

Symptom: Topology names that are 32 bytes long are not handled correctly on bootup.
Conditions: This issue is observed when 32-byte topology names are used.
Workaround: Use topology names that are shorter than 32 bytes.

Symptom: When an L3 port that is configured with the `ip igmp join-group` command is converted into an L2 port, multicast traffic is punted to the CPU.
Conditions: This issue is observed when the L3 port has `ip igmp join-group` configured for a group for which there are multicast sources. Later, the L3 port is converted into an L2 port participating in a VLAN that is either a source or receiver of that group.
Workaround: Apply one of the following workarounds:
- Remove the `ip igmp join-group` configuration before converting the port to an L2 port.
- Convert the L2 port back to an L3 port, remove the `ip igmp join-group` configuration, and then convert the port back to an L2 port.

Symptom: The IPv6 PIM register fails after an SSO. This results in S and G multicast routes disappearing from the last hop router (LHR). Because of this condition, traffic flow stops abruptly.
Conditions: This issue is observed after an SSO.
Workaround: There is no workaround. The LHR must be reloaded to fully restore the original condition.

Symptom: When the file descriptor reaches the maximum threshold limit, you cannot save the configuration or perform any file system-related operation because file descriptors are exhausted. The `File table overflow` error is displayed.
Conditions: This issue is observed on running the `dir/recursive <>` command periodically using the ANA tool.
Workaround: Do not run the `dir/recursive <>` command if leaks are detected. In addition, if the command is running through ANA server polling, disable it.

- CSCtk02647
  Symptom: On an LNS that is configured for L2TP aggregation, per-user ACLs downloaded through RADIUS might cause PPP negotiation failures (that is, IPCP is blocked).
  Conditions: This issue is observed when the LNS multilink is configured and negotiated for PPP/L2TP sessions, and per-user ACLs are downloaded for PPP users through RADIUS.
  Workaround: There is no workaround.

- CSCtk12608
  Symptom: Route watch fails to notify the client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.
  Conditions: This issue is observed on certain router configurations.
  Workaround: Use static routes that are associated with a specific interface.

- CSCtk47891
  Symptom: Traffic might be lost when the LC is reset.
  Conditions: This issue is observed when Fast Reroute (FRR) is configured and it is in active state when the LC is reset.
  Workaround: There is no workaround.

- CSCtk53463
  Symptom: To configure the `shape average cir_value bc_value` command, `bc_value` is limited by 4 milliseconds x `cir_value`. The 4 milliseconds represent the minimum interval time for bursts. However, the ES LC can support an interval value that is faster (that is, has a smaller interval) than 4 milliseconds. This is not the expected behavior for ES LC.
  Conditions: This issue is observed when the interval time for the `shape` setting is restricted from dropping below 4 milliseconds.
  Workaround: There is no workaround.

- CSCtl08601
  Symptom: Unconfiguring the DHCP pool causes the console to stop responding.
  Conditions: This issue is observed when the `no service dhcp` command is run before the pool is unconfigured.
  Workaround: There is no workaround.

- CSCtd54703
  Symptom: When the tunnel interface of a spoke is shut down and then restarted, the router crashes.
  Conditions: This issue is observed when the IPv6 NHRP cache fails and the tunnel interface of a spoke is shut down and restarted.
  Workaround: There is no workaround.

- CSCtk53606
  Symptom: When the router is inserted either as a probe source or a responder, a high maximum RTT value is seen for the UDP Jitter probe.
  Conditions: This issue is observed when running UDP Jitter probes.
  Workaround: There is no workaround.
Caveats in Cisco IOS XE 3.2S Releases

- **CSCtj85638**
  Symptom: Following a change to an ACL or prefix-list referenced by an OSPF `distribute-list...in` command, OSPF routes may be lost from the RIB.
  Conditions: This issue is observed in configurations that use a distribute list to filter routes that OSPF installs in the RIB.
  Workaround: Allow at least 10 seconds between successive changes to the ACL or prefix-list.

- **CSCth69364**
  Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.
  Cisco has released free software updates that address this vulnerability.

- **CSCti80847**
  Symptom: In a DVTI EzVPN setup, if the client sets the peer address to the secondary IP address of a loopback interface on the server, then the established IPSEC tunnel will not have the correct MTU value.
  Conditions: This issue is observed when the secondary IP address of the loopback is used as the IPSec tunnel end address.
  Workaround: Do not use the secondary IP address of the loopback as the IPSec tunnel end address.

- **CSCtb89745**
  Symptom: RRI functionality does not work as expected.
  Conditions: This issue is observed when the router is running in the HA Pair mode.
  Workaround: Add the crypto ACL again to populate the IP routes.

- **CSCti79478**
  Symptom: The serial interface is not attached to the OSPF process after reload even though there is a network statement to cover the interface.
  Conditions: This issue is observed when the serial interface is configured as an unnumbered interface.
  Workaround: Remove the `ip unnumbered` configuration, and then reapply it for the interface.

- **CSCtf71673**
  Symptom: A PRE crash occurs because of memory corruption caused by a block overrun.
  Conditions: This issue is observed when the router is configured for PTA and L2TP access and the router receives a PADX packet whose actual length is more than the length given in `pppoe_header`.
  Workaround: There is no workaround.

- **CSCta11223**
  Symptom: The router may crash when the `show dmvpn` or `show dmvpn detail` command is run.
  Conditions: This issue is observed when DMVPN is configured and the `show dmvpn` or `show dmvpn detail` command is run multiple times.
  Workaround: There is no workaround.

- **CSCtk12018**
  Symptom: The ESP crashes when a tunnel interface is recursively shut down and restarted.
Conditions: This issue is observed when the tunnel interface is recursively shut down and restarted.
Workaround: There is no workaround.

- CSCtl59149
  
  Symptom: When the Idle Peer Detect (IPD) feature is configured on an IPSec session, failover of the ESP may not be stateful. Some IPSec sessions may be torn down and re-created during the failover.

  Conditions: This issue is observed when the IPD feature is configured on the IPSec session.
  Workaround: There is no workaround. Note that the IPSec sessions that are torn down start up automatically after the failover of the ESP.

- CSCto88686
  
  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.


Open Caveats—Cisco IOS XE Release 3.2.0S

This section documents unexpected behavior that might be seen in Cisco IOS XE Release 3.2.0S.

- CSCth03302
  
  After RP switchover, IPv6 traffic on RB E subinterface recovers after few seconds.
  
  This condition has been observed when IPv6 is configured on RBE VCs and RP switchover has occurred.
  
  Workaround: There is no workaround.

- CSCth08313
  
  IPC Periodic Timer Driver MSG error has been observed on the Cisco ASR 1000 Router.
  
  The following error message has been seen during online operations:

  | IPC: Sending Big IPC msg to Driver MSG: ptr= 0x152CDAC8, flags= 0x14328, retries= 1, seq= 0x2016C68, refcount= 2, rpc_result = 0x0, data_buffer = 0x14FB3084, header = 0x78730658, data = 0x78730678 | HDR: src= 0x216001E, dst= 0x2010000, index= 0, seq= 27752, sz= 1808, type= 14209, flags= 0x1608, ext_flags= 0x0, hi= 0x1B622B, lo= 0x36C456 |

  Or
  
  | IPC: %SYS-SP-2-GETBUF: Bad getbuffer, bytes= 24616, process= "IPC Periodic Timer", ipl= 0, pid= 24, trace= 8174F8 81D19E8 8BEAD94 8BE85C4 853BAD4 8527704 854CE24 82AE180 82AE2EF 855E454 835AFD0 83552E8 |

  This has been seen either after boot of the router or after failover.

  Workaround: There is no workaround.

- CSCth11310
IP-subscriber sessions stop forwarding traffic after RADIUS proxy resets them. The session does not appear to get any traffic, and drops may be observed when the following command is used:
show platform hardware qfp active statistics drop
This behavior may occur on ASR 1000 Router Series, with routed IP-subscriber sessions that are reset and converted to RADIUS proxy sessions.
Workaround: There is no workaround.

- **CSCth14949**
  After enabling ip tcp header-compression when POS is configured on the interface a traceback has been seen.
  This condition may occur only when POS is configured on the interface and ip tcp header-compression enabled.
  Workaround: Do not enable ip tcp header-compression when POS is configured on the interface.

- **CSCth22250**
  On 2RU-F and ESP-5 when bringing up translations at higher rate, all sessions cannot be established.
  This condition has been observed on 2RU-F and ESP-5 when bringing up translations at higher setup rate.
  Workaround: Is to lower the setup rate.

- **CSCti03323**
  It takes the ESP about 1 minute longer to become fully active after an ISSU load version event.
  This only occurs during ISSU process and increases with more linecards.
  Workaround: There is no workaround.

- **CSCti14975**
  Tracebacks may be seen on Cisco ASR 1006 with RP2 while removing any security ACL.
  A failure may be observed when issuing the “show access-list” command while running Cisco IOS XE 3.2.1S release.
  This condition may occur when traceback is seen when unconfiguring a security ACL on RP2.
  A failure may be observed with ACLs on per-user sessions at 3K and 32K.
  Workaround: The router works normal, just traceback is seen.
  For now, do not issue “show access-list” command.

- **CSCti17802**
  The following log message may be incorrectly displayed to prompt the user to issue 'issu runversion' in cases where the ISSU upgrade has been aborted due to the following error:

  ISSU_PROCESS-SP-7-DEBUG: Peer state is [ STANDBY HOT ]; Please issue the runversion command

  Wrong message is shown when ISSU gets aborted after 'issu loadversion'.
  Workaround: No workaround. This behavior has no functional impact.

- **CSCti22164**
  ATM PVC with AC are up for ima-acr interface even if the controller is down.
This condition may occur when ATM PVC and attachment circuit are up for the ima-acr interface even though the controller is down for the IMA-ACR interface. The controllers are down as there is mismatch for the channel/port on the peer.

Workaround: No Workaround

- CSCti27214
  BFD with Routing flap, packet loss maybe seen on Standby RP.
  This may occur when the standby RP is booting up.
  Workaround: Disable both QoS (containing NBAR) and NBAR protocol discovery from all interfaces.

- CSCti31070
  Traceback may occur while performing downgrade to a lower version of image.
  This instance has been observed after issuing `runversion` while performing downgrade to a lower version of image.
  Workaround: There is no workaround.

- CSCti34437
  QFP Tracebacks are seen after switchover for an active SRTP call.
  This condition has been observed during Switchover with SIP-SIP and SRTP-SRTP basic audio calls.
  Workaround: There is no workaround.

- CSCti50692
  ESP may reload when activating 4 template services.
  This condition has been observed when the following steps have occurred:
  1. Activate template service A in one CoA.
  2. Activate services B, C and D in another CoA.
  3. Loss of connectivity on the ESP may occur when activating template services.
  Workaround: There is no workaround.

- CSCti53718
  Newly added StandbyESP is unable to activate during init state, after performing “issu runversion” command.
  This condition has been seen when bringing up 2 pppoea sessions and performing “issu runversion” command.
  Workaround: There is no workaround.

- CSCti59758
  Distributed SBC reserves transcoding resources for a non-transcoded call.
  This symptom is observed on distributed SBC on the ASR 1000 platform with DSP-SPA when SDP includes rtpmap and ptime information.
  Workaround: There is no workaround.

- CSCti59760
Under Cisco ASR 1000 Router B2B inter-chassis application redundant mode for CUBE-SP, it is seen that not all SBC related configuration changes made on the Active device gets auto-sync'd to the running-config on the Standby Device. Some examples of this are add/delete/edit of adjacency config and add/delete/edit of CAC and call policies. Thus the running-config between the Active and Standby devices may be out-of sync. If running-config is saved to the startup config this can result in discrepancies between the startup-config on the Standby device and startup config on the Active device.

Although this discrepancy in the replication of SBC config does affect the running-config on the Standby device, it will NOT affect the accuracy of the Standby device upon application failover. Running-config is not used by the Standby device under scenario of application failover, only upon bootup. Application failover will execute successfully.

This has been seen when CLI edits for SBC performed on the Active device under inter-chassis HA mode of CUBE-SP application.

Workaround: This issue does not affect the functionality of SBC upon application failover, only the accuracy of the SBC running-config on the Standby device. Workaround is to manually insert startup config on the Standby device w/ accurate reflection of Active SBC config rather than writing running-config to startup-config, which could inadvertently result in inaccurate SBC config upon reboot.

- CSCti63058
  The CPS rate for Generic LAC and LNS sessions is about 5% less than what we had in prior releases.
  This is specific to Generic LAC and LNS while bringing up the sessions in a specific setup.
  Workaround: There is no known workaround.

- CSCti65517
  DSP SPA may not activate after proper bootup if HOT inserted into ASR 1000 SIP-X line-card following removal of a previously inserted with active SPA from the same subslot.
  Error looks similar to the example, below:
  Aug 30 15:24:37.020: %DSP-3-TIMER: SIP0/3: Bootp timer expired for DSP 0
  ......
  This condition is seen under hot SPA OIR scenario, if an active SPA is removed from an ASR1k SIP-X line-card and replaced by DSP SPA, the DSP SPA may not activate after proper bootup.
  Workaround: Reload the SIP-X line-card via cli: “hw-module slot <slot-num>”.

- CSCti70703
  The ASR 1000 Router may reload when multiple H.323 calls made through ZBFW.
  This has been seen when ZBFW configured to inspect H.323 traffic and multiple H.323 calls are going through the system.
  The root cause analysis showed that this issue can happen with NAT configuration. also.
  Workaround: There is no workaround.

- CSCti70743
  Under B2B inter-chassis HA scenario for CUBE-SP while using SBC application, after execution of RCP to copy files to and from the Cisco ASR 1000 chassis may result in trigger of application failover.
  This condition is seen under inter-chassis HA with B2B scenario for CUBE-SP while using SBC application along with execution of 'copy rcp:... local-loc'.
Workaround: There is no workaround.

- CSCti71739
  Rekey is not getting to the Cisco ASR 1000 Router from GETVPN KS.
  This may happen when the ASR 1000 Router's and GM's are connected back to back.
  Workaround: There is no workaround.

- CSCti75302
  RP failure (during Punt Keepalive process) is observed after a longevity Test with BGP, OSPF, and Multicast configurations.
  This conditions has been observed after a longevity test. This problem has been identified as a possible ESP memory leak which would may cause Active RP to crash (RP1 and RP2), and due to this leak the RPs may continue to have failures every three hours causing a network outage.
  In addition, there are multiple scale features enabled at the time of failure which includes 200 BGPv4 sessions, 800 OSPF sessions, 500 IGMPv2 groups with PIM and 50 RSVP sessions.
  Workaround: There is no workaround.

- CSCti80847
  In a dVTI + EZVPN setup, if client sets the peer address to the secondary ip address of a loopback interface on the server, then the established IPSEC tunnel will not have the correct MTU value.
  This is not a very common configuration, one primary address is sufficient to support multiple clients. There is no need to use the secondary address for this case.
  The existing ASR implementation uses the ip MTU of the tunnel source interface as the base of the IPSEC MTU. If client set peer to a secondary ip address on server, then MTU is mistakenly set based on a large default value, instead of base on the correct tunnel source interface.
  Workaround: Do not use secondary ip of loopback as ipsec tunnel end address.

- CSCti87639
  Standby RP reloads due to config out of sync or keepalive failure in RPR mode.
  This condition may occur when Standby RP reloads due to keepalive failure in RPR mode. This issue is observed while running nbar scripts or sometimes even with no activity on box. It cannot be reproduced manually.
  Workaround: Operate in SSO mode.

- CSCtj02412
  On the Cisco ASR 1000 Router configured with the following:
  1. Three policy maps: P1, P2, P3.
  2. Policy map P1 is applied under multilinkPPP interface. P2 and P3 not applied under any interface.
  3. Policy map P2 has one class which matches protocol.
  4. While configuring P2 as a child policy of P3 gives an error:
     The following error may appear on the console: NBAR is not supported on Multilink1.
     This problem occurs only when P1 has already applied under multilinkPPP interface and P2 has one class which matches protocol (NBAR).
     Workaround: Remove P1 from multilinkPPP interface, then configure P2 as child policy of P3. Now apply P1 under multilinkPPP.
- **CSCti96774**
  Inbound ACL will be deleted from session.
  This condition is observed when performing CoA after applying an outbound ACL to the same session (with IPv6 and av-pair configured on the router).
  Workaround: Re-apply inbound ACL or in and out at the same time.

- **CSCtj05507**
  Stale objects have been seen when SSO is configured on an Cisco ASR 1000 Router.
  Workaround: There is no workaround.

- **CSCtj05670**
  When doing SSO with scaled mLDP configuration, path set for some of the VRFs are not configured.
  This issue only occurs when configuring mLDP on 100 VRFs with 100 receivers.
  Workaround: There is no workaround.

- **CSCtj12161**
  Validation of SIP message header may cause loss of activity on the Cisco ASR 1000 Router Series, intermittently.
  This condition may be seen when simulate SIP calls between SIP client and SIP server (Cisco ASR 1000 Router Series).
  For example:
  ```
  Validation of SIP invite message header sent fails
  Validation Failed <<< NT/OR is NOT FOUND on Side B
  ```
  Workaround: There is no workaround.

- **CSCtj14778**
  H323 call setup may lose connection for 1000+ consecutive calls.
  This has been observed when H323 call setup is configured for 1000+ consecutive calls.
  Workaround: Clear nat translations in UUT and the next 1000 calls would pass. In addition, by reducing the nat TCP timeout value (for example: 5 min) will resolve this issue.

- **CSCtj15181**
  SMAND reloads when issuing "**sh policy-map type inspect zone-pair**" command.
  Workaround: Use HSL for retrieving zone-pair information.

- **CSCtj18999**
  ESP reloads with 13.5k concurrent sip calls without RTP and with CPS=2k in NAT only configuration.
  Workaround: Use less CPS.

- **CSCtj23259**
  The ASR 1000 Router acts as a PE and has scaled configs for L2TPv3 feature combination with EoMPLS and ATMoMPLS with 2000 Pseudowires. CC failure is observed when doing CC OIR.
  This condition may occur when doing CC OIR and the CC failure is observed. This maybe seen only when the SIP is using SPA-1XCHOIC12/DS0 or SPA-2XOC3-POS spa’s on the router. This has not been observed with other types of SPAs.
Workaround: There is no workaround.

- **CSCtj30897**
  Alterations made to dspfarm resources (without first de-activating SBC application) for **maximum sessions** can cause SBC to stop processing new transcoded calls and also SBC does not apply the newly configured changes immediately.
  This condition has been observed when alterations to **dspfarm profile x transcode** without first de-activating SBC application can cause SBC to stop processing new transcoded calls.
  Workaround: De-activate SBC application (via `no activate cli`) prior to making any changes to dspfarm resources. If this is done, upon re-activation of SBC, dspfarm changes will be applied immediately and SBC will process new incoming transcoded calls without issue.

- **CSCtj30936**
  H.323 to SIP interworking performance degradation.
  This instance is observed with CPS=29/CHT=180 on Cisco ASR 1006 RP1 with ESP-10, there is TCP connection setup failure between H.323 endpoint and the ASR 1000 Router, thus causes H323 to SIP calls failure.
  Workaround: There is no workaround.

- **CSCtj31470**
  Multicast ping failure may occur when complex CEF options are on.
  The detailed command is **“ip cef accounting per-prefix non-recursive prefix-length load-balance-hash”**.
  This condition has been observed when the ASR 1000 Router is using 12.2(33)XNE image.
  Workaround: There is no workaround.

- **CSCtj35914**
  In a setup with primary CEM PW and a backup configured, the traffic flows in the backup path when the primary is still up.
  This condition has been observed when reloading the module on the peer PE, when the primary path and controller is down. Allow the back up path to come up when primary path is still down. Bring up the primary path now, the traffic will not be switched to the primary path, it still flows in the back up path, though the primary path is up.
  The traffic does not switchover to primary, even if the back up path goes down.
  Workaround: Reset the module on the peer PE again when the primary controller / path is up.

- **CSCtj42023**
  Tracebacks with cef-mpls debug enable and disable failure may occur with sip calls.
  This condition has been observed when enabling and disabling after initiating the following:
  “debug platform hardware qfp active feature cef-mpls datapath ip all”
  Workaround: Do not send bulk traffic after enabling debug.

- **CSCtj43730**
  When QFP failure has occurred the call is lost and the ESP may reload.
  This condition has been observed in a environment with SRTP - SRTP calls.
  Workaround: There is no workaround.

- **CSCtj44326**
When issuing “show platform hard slot p0 fan status” command the following message for the fan speed is incorrectly shown on the console:

Fan group 1 speed: 166%
Fan group 2 speed: 6%
Fan 0: Normal

This instance maybe seen when issuing “show platform hard slot p0 fan status” command on the 1RU.

Workaround: Is to issue “show environment all” command on the 1RU. This will provide an accurate output for current fan speed. Fan failures will be correctly defined when issuing “show facility-alarm status” command.

- CSCtj47086
  When a connected route that is also owned by EIGRP or OSPF is replicated from one routing table to another, any route-map that is applied after redistributing the route into EIGRP may not perform properly if the source specified during redistribution is anything other then connected (that is, EIGRP or OSPF).

Workaround: Make sure to specify the source as EIGRP or OSPF instead of connected when redistributing the replicated routes.

- CSCtj52969
  The following message may be observed when issuing the “show issu state detail” command after performing an issu loadversion operation:

  %ISSU_PROCESS-3-IPC_AGENT: Failed to send; error code [ timeout ]

  This message may be observed when issuing the 'show issu state detail' command after performing an 'issu loadversion' operation.

  Workaround: There is no workaround.

- CSCtj55459
  No configuration seen or configuration has not taken into effect while configuring “ip nbar protocol-discovery” on the interfaces, only once on multiple interfaces. Except on the first interface the configuration is not seen, and on the rest of them.

  This condition may occur when the configuration is done through a script that allows for multiple interfaces to be configured in a single task and at the same time.

  Workaround: There is no workaround.

- CSCtj55916
  The ESP reloading was seen in different scenarios due to fman_fp core:
  - interface flapping
  - config/un-config interface
  - RP switchover with scalability config - 8k PVCs

  The issue could be seen in the following cases:
  - interface flapping
  - config/un-config interface
  - RP switchover with scalability config - 8k PVCs

  Workaround: The router should automatically recover after the ESP reloading.

- CSCtj57211
When exceeding the maximum session configured in a dspfarm the uSBC will reply to new call setup with SIP 500 error message, as opposed to SIP 503.

This has been observed when configuring multiple dspfarm and attempt to place more calls than defined in the maximum session parameter of a dspfarm.

Workaround: Use only one dspfarm.

- CSCtj58686
  The subclassification numbers for “match protocol kazaa2 file-transfer” are different for the same traffic over server port 80 and port non80.

Workaround: There is no workaround.

- CSCtj61454
  A problem may occur when provision under codec system and is unable to be deleted.

This problem is observed when provision under codec system is active after deletion.

Workaround: There is no workaround.

- CSCtj64755
  Console may not activate for 4-5 mins when ima configs are removed from the virtual controller with scale.

This condition has been observed when ima interface is configured for scale.

Console may not activate when removing ima config from virtual controller “no vtg 1 t1 ima-group”.

Workaround: There is no known workaround.

- CSCtj70493
  On the Cisco ASR 1001 versions supported as of IOS XE 3.2.0S during BGP Convergence times are slower than expected.

  **Note**  
  BGP Convergence does occur in all cases.

This condition is seen during scaled configurations and becomes more apparent as BGP peer configured on the ASR1001 per peer increases.

Workaround: There is no workaround at this time.

- CSCto03123
  Symptoms:
  1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
  2. Additional memory leak can occur when frequent sensor value changes take place.

  Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.
If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
Caveats in Cisco IOS XE 3.1S Releases

This chapter provides information about caveats in Cisco IOS XE 3.1S releases. Because Cisco IOS XE 3S is based on Cisco IOS XE 2 inherited releases, some caveats that apply to Cisco IOS XE 2 releases also apply to Cisco IOS XE 3S. For a list of the software caveats that apply to Cisco IOS XE 2, see the “Caveats for Cisco IOS XE Release 2” section at the following location:


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


This chapter contains the following section:

• Caveats in Cisco IOS XE 3.1S Releases, page 403

Caveats in Cisco IOS XE 3.1S Releases

Caveats describe unexpected behavior. 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 this chapter.

This section describes caveats in Cisco IOS XE 3.1S releases.

In this section, the following information is provided for each caveat:

• Symptom—A description of what is observed when the caveat occurs.

• Conditions—The conditions under which the caveat has been known to occur.

• Workaround—Solutions, if available, to counteract the caveat.

Note

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)
The Dictionary of Internetworking Terms and Acronyms contains definitions of acronyms that are not defined in this document:

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

This section consists of the following subsections:

- Resolved Caveats—Cisco IOS XE Release 3.1.4aS, page 404
- Open Caveats—Cisco IOS XE Release 3.1.4S, page 405
- Resolved Caveats—Cisco IOS XE Release 3.1.4S, page 406
- Open Caveats—Cisco IOS XE Release 3.1.3S, page 416
- Resolved Caveats—Cisco IOS XE Release 3.1.3S, page 420
- Open Caveats—Cisco IOS XE Release 3.1.2S, page 430
- Resolved Caveats—Cisco IOS XE Release 3.1.2S, page 433
- Open Caveats—Cisco IOS XE Release 3.1.1S, page 449
- Resolved Caveats—Cisco IOS XE Release 3.1.1S, page 455
- Open Caveats—Cisco IOS XE Release 3.1.0S, page 460

**Resolved Caveats—Cisco IOS XE Release 3.1.4aS**

The following are the resolved caveats in Cisco IOS XE Release 3.1.4aS:

- **CSCtq96329**
  
  Symptoms: Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can happen only when bgp deterministic-med is configured. The following releases are impacted:
  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the `no bgp deterministic-med` command and then the `clear ip bgp *` command or hardreset of BGP session to remove any stale prefixes.

  It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

  Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- **CSCtr22007**
  
  Symptoms: A Cisco 7600 router that is configured with RSVP crashes.

  Conditions: MPLS-TE Tunnel Flap.

  Workaround: There is no workaround.
Open Caveats—Cisco IOS XE Release 3.1.4S

The following are the open caveats in Cisco IOS XE Release 3.1.4S:

- **CSCtg59243**
  Symptom: The Hot ICE Before After feature stops working when you run the `mpls static binding ipv4` LDP command.
  Conditions: This issue is observed when you run the `mpls static binding ipv4` command.
  Workaround: There is no workaround.

- **CSCto49680**
  Symptom: On a traffic class that is fitted with a time-range access list, the traffic keeps meeting the matching criteria even when the access list is inactive.
  Conditions: This issue is observed a few days after a traffic class is fitted with a time-range access list.
  Workaround: There is no workaround.

- **CSCtq56709**
  Symptom: The Cisco ASR 1000 ESP reloads automatically.
  Conditions: This issue is observed on an ISG under high-load conditions.
  Workaround: There is no workaround.

- **CSCto77352**
  Symptom: The standby RP cannot reach the hot synchronization state with the active RP. The standby RP continues to reload automatically, and the following message is displayed:
  
  *Apr 18 15:38:47.704: %SYS-3-CPUHOG: Task is running for (3305)msecs, more than (2000)msecs (1/1), process = IPC Dynamic Cache.*
  
  Conditions: This issue is observed in the stateful switchover (SSO) mode, when the ISG is configured as the DHCP server, and the DHCP lease time is set to a low value.
  Workaround: There is no workaround.

- **CSCtn62287**
  Symptom: The standby router may crash when an interface flaps or while performing a soft OIR of the SPA.
  Conditions: This issue is observed when interfaces are bundled as a multilink and traffic is flowing across the multilink.
  Workaround: There is no workaround.

- **CSCtq86244**
  Symptom: After an SSO, ISIS does not send its topology database to the TE. Therefore, the TE cannot determine the path to the destination of the tunnels and the tunnel stays down.
  Conditions: This issue is observed when the ISIS is configured with the `nsf cisco` command and the TE is not configured for high availability.
  Workaround: Run the `nsf ietf` command on the ISIS.
Caveats in Cisco IOS XE 3.1S Releases

- **CSCtq96329**
  
  **Symptoms:** Router fails to send withdraws for prefixes, when “bgp deterministic-med” is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  **Conditions:** This symptom can happen only when “bgp deterministic-med” is configured.

  The following releases are impacted:
  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  **Workaround:** Disable deterministic med in the network/AS by issuing the `no bgp deterministic-med` command and then the `clear ip bgp *` command or hardreset of BGP session to remove any stale prefixes.

  It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

  **Further Problem Description:** If deterministic med is enabled, withdraws are not sent.

- **CSCtr26226**
  
  **Symptoms:** The RP and SIP crash.

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

  **Workaround:** There is no workaround.

**Resolved Caveats—Cisco IOS XE Release 3.1.4S**

The following are the resolved caveats in Cisco IOS XE Release 3.1.4S:

- **CSCtb24959**
  
  **Symptom:** The router may crash while a large number of RP mappings are being cleared.

  **Conditions:** This issue is observed when you configure the router as an RP agent and candidate RP for a large number of RPs. The router may crash when you run the `clear ip pim rp-map` command multiples times.

  **Workaround:** Do not run the `clear ip pim rp-map` command multiples times.

- **CSCth90147**
  
  **Symptom:** The router responds to a router solicitation message with a router advertisement message.

  **Conditions:** This issue is observed when you run the `ipv6 nd ra suppress` command. This command is only intended to suppress periodic multicast router advertisement messages. The router continues to respond to unicast router solicitation messages, which is the intended behavior.

  **Workaround:** Use an ACL to block the reception of router solicitation packets.

- **CSCti87194**
  
  **Symptom:** When a long IPC message is fragmented, the last fragment causes a crash because of an invalid zone value.

  **Conditions:** This issue is observed when a long IPC message is fragmented.
Caveats in Cisco IOS XE 3.1S Releases

OL-23288-23

Workaround: There is no workaround.

- CSCti91029
  Symptom: A traceback occurs, and the following message is displayed:
  %INFRA-3-INVALID_GPM_ACCESS: Invalid GPM ...
  Conditions: This issue is observed when NAT configuration commands or NAT EXEC commands are run after the `debug ip nat aclnum` command is run.
  Workaround: There is no workaround.

- CSCtj20776
  Symptom: When a RADIUS proxy session is reauthenticated, the Accounting Stop record is sent for the session.
  Conditions: This issue is observed when all the following conditions are met:
  - The authentication request comes from the AP.
  - The accounting request comes from the AZR, and the session on the ISG is associated with the AZR.
  - The ISG receives a reauthentication request from the AP.
  - The acct-terminate-cause field in the Stop record is set to none.
  The Accounting Stop record is sent for the RADIUS proxy session and the services under the session. However, note that the RADIUS proxy session is still active and a Stop record is not sent for the session when the session is cleared.
  Workaround: There is no workaround.

- CSCtj30155
  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:
  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload
  Cisco has released free software updates that address these vulnerabilities.
  Workarounds that mitigate these vulnerabilities are available.

- CSCtj44374 and CSCti70931
  Symptom: When you try to configure the router through Telnet access (vty), the router stops responding. The console is active, but not responsive. When the `show processes cpu` command is run, the output shows high CPU utilization.
  Conditions: This issue is observed when you configure 200 or more call policy sets, with each policy set containing a large number of entries.
  Workaround: Do not create more than 100 entries in each call policy set.

- CSCtj58672
  Symptom: The MallocLite memory leak occurs when the `vlan_bl_util_process_bitlist` function is called.
Caveats in Cisco IOS XE 3.1S Releases

Conditions: This issue is observed when the L3VPN and BFD profile configuration is set on the router.
Workaround: There is no workaround.

- CSCtj87846
  Symptom: A subinterface that is in the Up state is considered to be in the Down state by the PfR master controller.
  Conditions: This issue is observed under either of the following conditions:
  - A subinterface is used as an external interface and the corresponding physical interface goes down and then comes up.
  - The router is reloaded.
  Under either condition, the PfR master controller is not notified that the subinterface has returned to the Up state.
  Workaround: Run the `clear pfr master *` command on the PfR master controller.

- CSCtj92247
  Symptom: The standby RP reloads automatically because the configuration is not in synchronization with the primary RP.
  Conditions: This issue is observed when you modify the parameters, for example, the peak value, of a VP.
  Workaround: There is no workaround.

- CSCtk76697
  Symptom: After a test crash on a line card, the first 100-odd service instances out of 4000 service instances on the line card change to the Down state. This results in a complete traffic drop on these service instances.
  Conditions: This issue is observed only during the first test crash on the LC after the router is booted.
  Workaround: Run the `shut` and `no shut` commands on the service instance or the interface.

- CSCtl67150
  Symptom: PPP multilink interfaces do not come up on the serial interface.
  Conditions: This issue is observed when all the following conditions are met:
  - T1 channel groups are created in a CT3 interface.
  - A multilink interface is created.
  - One link is created per channel group.
  - CHAP authentication is applied when PPP encapsulation is used for each link.
  Workaround: There is no workaround.

- CSCtl84797
  Symptom: SBC traceback occurs.
  Conditions: This issue is observed when Lawful Intercept (LI) is enabled and there are multiple media sessions in a single call, that is, SDP contains information about multiple media sessions.
  Workaround: There is no workaround.

- CSCtn15317
Symptom: Traffic on the MPLS VPN is dropped. The LFIB entry on the P router contains an instruction to TAG all the packets that are destined for the PE router instead of the POP instruction that is expected on a directly connected P router.

Conditions: This issue is observed when all of the following conditions are met:
- The ISIS protocol is running as IGP on MPLS infrastructure.
- ISIS on the PE router is a summarizing network that includes the BGP VPNv4 Update Source configuration.
- The P router is running an MFI-based image.

Workaround: Remove the `summary-address` configuration from ISIS on the PE router, and change the BGP update source.

- **CSCtn19178**

Symptom: If you are running an Inter-AS MPLS design across two autonomous systems, the router may clear the local label for a working VRF and a new local label is not reassigned.

Conditions: This issue is observed on the MPLS Edge LSR when you remove the configuration of an unused VRF, including either of the following:
- The VRF interface, for example, by running the `no interface Gi1/0/1.430` command.
- The same VRF process, for example, by running the `no router ospf process-id vrf vrf-name` command.

Run the `show ip bgp vpnv4 vrf A subnet` command on the working VRF to verify whether you are facing this issue.

Workaround: To reprogram a new local label on the PE router, clear the MP-BGP session by using one of the following commands:
- `clear ip bgp mp-bgp neighbor soft in clear`
- `ip bgp mp-bgp neighbor soft out`

- **CSCtn2728**

Symptom: When the `exit` command is run in the EVC mode, the standby RP may reload automatically due to configuration synchronization and the following error message may be displayed:

```
%PFREDUN-SP-STDBY-6-STANDBY: Ready for SSO mode   Config Sync: Line-by-Line sync verifying failure on command: exi exi due to parser return error rf_reload_peer_stub: RP sending reload request to Standby. User: Config-Sync, Reason: Configuration mismatch
```

Conditions: This issue is observed when an unsupported interface CLI option is used with the `destination` keyword in the ERSPAN source session configuration.

Workaround: There is no workaround. Do not run commands such as the `exit` command that are not applicable to the EVC mode.

- **CSCtn38996**

Symptom: MVPN traffic is lost when a peer is reachable using a TE tunnel and an interface flap is performed to enable the selection of the secondary path. The multicast route does not contain a native path that uses the physical interface.

Conditions: This issue is observed when the `mpls traffic-eng multicast-intact` command is configured under OSPF.

Workaround: Run the `clear ip ospf process` command on the core router.
• CSCtn48009
Symptom: A Cisco ASR 1000 series router may experience unexpected periodic ESP reloads at regular intervals (that is, every X hours and Y minutes). The issue is specific to an ESP such that the problem will follow that ESP if moved to a different slot and/or chassis. Note that Cisco IOS images with this change will still experience periodic reloads although the reporting will more clearly indicate the cause.
Conditions: This symptom is observed with any Cisco ASR 1000 series router with a persistent error in the QFP memory.
Workaround: There is no workaround. The affected ESP board or the Cisco ASR 1001 router must be replaced.

• CSCtn53222
Symptom: Real servers, such as ASNGW, GGSN, and RADIUS, are stuck in the READY_TO_TEST state and do not switch to the OPERATIONAL state.
Conditions: This issue is observed when a real server moves to the FAILED state because of real server failure that is detected by the inband failure mechanism. After the retry timeout interval, the real server is moved to the READY_TO_TEST state.
Workaround: Change the state of the real server to OUTOFSERVICE and then to INSERVICE.

• CSCtn56526
Symptom: The MBS is always calculated on the basis of the MTU value. The user-defined MBS value is not included in the output of the show atm pvc command.
Conditions: This issue is observed when the MBS is configured using the CLI and the show atm pvc command is run.
Workaround: There is no workaround.

• CSCtn64500
Symptom: Multicast traffic does not pass through an ATM point to a multipoint subinterface.
Conditions: This issue is caused by an incomplete inject of a P2MP multicast adjacency on an ATM P2MP interface. The output of the show adjacency atm interface detail command shows that the inject P2MP multicast adjacency is in an incomplete state.
Workaround: Run the clear adjacency command to force-repopulate the incomplete adjacency.

Note: Note that the clear adjacency command has a system-wide impact. As an alternative, you can use unicast commutation.

• CSCtn65599
Symptom: Some multicast streams from the CE router are not forwarded to the Data MDT by the PE router.
Conditions: This issue is observed after an SSO or a PRE crash.
Workaround: There is no workaround.

• CSCtn73941
Symptom: After performing an OIR for an ES card having EVC configuration with the module clear-config command enabled, restoring the old configuration does not work. This indicates that traffic will not be forwarded over those service instances. In addition, VLANs used in the previous configuration cannot be effectively used on those ports.
Caveats in Cisco IOS XE 3.1S Releases

Conditions: This issue is observed when you run the `module clear-config` command.
Workaround: There is no workaround.

- CSCtn74673
  Symptom: After a reload, incoming multicast traffic is punted into the CPU before MFIB is downloaded to the line cards. Because of the high CPU rate, the line cards are stuck in a continual loop of failing to complete the MFIB download.
  Conditions: This issue is observed when high CPU utilization is caused by the multicast traffic. The `show mfib linecard` command does not show the line cards in synchronization with each other and the tables are in the connecting state.
  Workaround: Reload the line cards.

- CSCtn95344
  Symptom: The standby RSP gets stuck in RF progression at cold bulk while booting.
  Conditions: This issue is observed after the RPR is downgraded from Release 12.2(33)SRE2 to Release 12.2(33)SRE1.
  Workaround: Reload the router.

- CSCtn96521
  Symptom: When the spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors are not able to establish an adjacency.
  Conditions: This issue is observed when the spoke peer group is configured before the iBGP peer group.
  Workaround: Configure the iBGP peer group before the spoke peer group.

- CSCtn74541
  Symptom: The BGP peer router crashes when the `clear bgp ipv4 unicast peer` command is run.
  Conditions: This issue is observed when all the following conditions are met:
  - Internal BGP is running between Router 1 and Router 2.
  - External BGP is running between Router 1 and Router 3.
  - Traffic is travelling from Router 3 to Router 2.
  - The `clear bgp ipv4 unicast peer` command is run on Router 2.
  Workaround: There is no workaround.

- CSCtn98642
  Symptom: The RP crashes, and the following error message is displayed:
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Ether-SPA background process
  Conditions: This issue is observed when QinQ (min 50) and QinQ-Any with the same outer VLAN is present and both the following conditions are met:
  - A large-scale configuration has QinQ and QinQ-Any with the same outer VLAN on SPA.
  - The router is reloaded.
  Workaround: There is no workaround.

- CSCto02448
  Symptom: The AS-PATH attribute is lost after an inbound route refresh is performed.
Conditions: This issue is observed when all the following conditions are met:
- The neighbor is configured with soft-reconfiguration inbound.
- The inbound routemap is not configured for the neighbor.
- The nonroutemap inbound policy (filter list) allows the path.

Workaround: Use the routemap inbound policy to filter the prefixes.

- CSCto03123
  Symptoms:
  1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
  2. Additional memory leak can occur when frequent sensor value changes take place.

Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

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

- CSCto07586
  Symptom: An IPv4 static BFD session does not get established on a system that does not have IPv6 enabled.

Conditions: This issue is observed when all of the following conditions are met:
- The router does not have IPv6 enabled.
- BFD is enabled on an interface.
- An IPv4 static route is configured with BFD routing through the interface.

The IPv4 BFD session does not get established, and as a result, the static route does not get installed.

Workaround: Unconfigure and then reconfigure BFD on the interface.

- CSCto07919
  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:
  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are available.

- **CSCto10336**
  Symptom: The LNS router stops responding at the interrupt level.
  Conditions: This issue is observed during control channel cleanup.
  Workaround: There is no workaround.

- **CSCto15361**
  Symptom: The Active Supervisor crashes when the `router eigrp` configuration is removed.
  Conditions: This issue is observed because the EIGRP Hello process is stopped while disabling the IPv6 router EIGRP.
  Workaround: Modify the `igrp2_procinfos_free` function to stop the EIGRP Hello process before cleaning up the peer list.

- **CSCto16106**
  Symptom: An address is not assigned when the `ip dhcp use class aaa` command is run.
  Conditions: This issue is observed when the DHCP server is configured to download a class name from the RADIUS server by using the `ip dhcp use class aaa` command and to lease an IP address from that class. The IP address is not assigned to the client.
  Workaround: There is no workaround.

- **CSCto31265**
  Symptom: The Area Border Router (ABR) does not translate Type 7 LSA when the primary Type 7 LSA is deleted, even if another Type 7 LSA is available.
  Conditions: This issue is observed when you are using OSPFv3 and the ABR receives multiple Type 7 LSAs for the same prefix from multiple ASBRs.
  Workaround: Perform one of the following steps:
  - Delete and then add the static route that generates Type 7.
  - Run the `clear ipv6 ospf force-spf` command on the ABR.
  - Run the `clear ipv6 ospf redistribution` command on the ASBR.

- **CSCto41165**
  Symptom: The standby router reloads automatically when you use the `ip extcommunity-list 55 permit | deny` command and then run the `no ip extcommunity-list 55 permit|deny` command.
  Conditions: This issue is observed when the standby router is configured.
  Workaround: There is no workaround.

- **CSCto44585**
  Symptom: Packets with the DF bit set across the L2TPv3 tunnel are punted or dropped on the CPU.
  Conditions: This issue is observed when the PMTU in the pseudowire class configuration is enabled.
  Workaround: Reduce MTU on the client side.

- **CSCto46716**
  Symptom: Routes over the MPLS TE tunnel are not present in the routing table.
  Conditions: This issue is observed when the MPLS TE tunnel is configured with forwarding adjacency. If you run the `debug ip ospf spf` command while the SPF process link for the TE tunnel is in its own RTR LSA, the `Add path fails: no output interface` message is displayed.
Note  Some tunnels are not affected when the MPLS TE tunnel is configured with the forwarding adjacency. However, it is not always possible to identify the tunnel that is affected. The number of affected tunnels increases with the number of configured tunnels.

Workaround: Use the **autoroute announce** command instead of the **forwarding-adjacency** command.

- CSCto52235
  Symptom: The MAC address accounting commands cannot be used.
  Conditions: There are no specific conditions under which this issue is observed.
  Workaround: There is no workaround.

- CSCto55643
  Symptom: High CPU loading conditions can result in delayed download of multicast routes to the line cards, resulting in the MFIB state on the line cards that are not in synchronization with the RP. The **show mfib linecard** command shows line cards in the Sync Fail state and the LOADED state.
  Conditions: This issue is observed when there is high CPU load due to router reload or line card OIR events in a highly scaled multicast environment with high line rates of multicast traffic and unrestricted process-switched packets.
  Workaround: There is no workaround.

- CSCto55983
  Symptom: After a reload, incoming multicast traffic is punted into the CPU before MFIB is downloaded into the line cards. Because of the high CPU rate, line cards are stuck in a continual loop of failing to complete MFIB download and retrying.
  Conditions: This issue is observed during high CPU utilization caused by multicast traffic. The **show mfib line summary** command does not show cards in synchronization.
  Workaround: There is no workaround.

- CSCto72480
  Symptom: The output of the **show mfib linecard** command shows that line cards are in the Sync Fail state.
  Conditions: This issue is observed when the last reload context displayed in the output of the **show mfib linecard internal** command is epoch change. This indicates that an IPC timeout error has occurred in the communications channel (MRIB), which downloads multicast routing entries to the MFIB. In this scenario, multicast routing changes are not communicated to the failed line cards and are not synchronized with the RP.
  Workaround: Run the **clear mfib linecard** command.

Note  The workaround may not work if high CPU utilization continues to be present and IPC errors are reported.

- CSCto74038
  Symptom: After an upgrade, the CESoPSN (clock) pseudowire stays in the Down state due to payload size value mismatch.
Conditions: Before upgrading, the payload size is configured to 80 and the dejitter value is the
default (5). This issue is observed if you configure the payload size or dijitter value to a value other
than the default and upgrade the system.
Workaroud: Set the payload size and dejitter value to their defaults.

• CSCtq09088
  Symptom: The router crashes while trying to run the `ip rsvp sender-host` command. For example:
  `ip rsvp sender-host 203.0.113.26 203.0.113.65 UDP 11 10 10 identity bogusID`
  Conditions: This issue is observed when the `ip rsvp sender-host` command is run.
  Workaroud: There is no workaround.

• CSCtf81249
  Symptom: Memory leaks are observed while running configuration commands.
  Conditions: This issue is observed only when the Tcl shell is used.
  Workaroud: Run the `end` command.

• CSCt90292
  Symptom: The following error messages are displayed:
  `an 18 08:00:16.577 MET: %SYS-2-MALLOCFAIL: Memory allocation of 9420 bytes failed from
  0x42446470, alignment 32  Pool: I/O Free: 11331600  Cause: Memory fragmentation
  Alternate Pool: None Free: 0  Cause: No Alternate pool -Process= "BGP I/O", ipl= 0,
  pid= 564  -Traceback= 417E8BEC 4180FA6C 42446478 42446864 42443984 40FC18C8 40FCCB4C
  40FD1964 403BDBFC 403BC34 40345050 403668AC`
  Conditions: This issue is observed when a large number of hits and failures are observed in the
medium buffers and all are of link-type IPC. For example:
  `buffer information for Medium buffer at 0x4660E964 ...  linktype 69 (IPC), enctype
  1 (ARPA), encsize 14, rxttype 0 if_input 0x481DEA50 (EOBC0/0), if_output 0x0 (None)`
  Workaroud: There is no workaround.

• CSCtq36726
  Symptom: Configuring the `ip nat inside` command on the IPSec dVTI VTEMP interface does not
have any effect on the cloned virtual access interface. The NAT feature does not work because the
virtual access interface does not get this command cloned from its corresponding VTEMP.
  Conditions: This issue is observed on a router with dVTI-based IKEv2 configured.
  Workaroud: Reconfigure the virtual template interface so that the `ip nat inside` command is applied
first.

• CSCtq83629
  Symptom: When an IPC error occurs, another error associated with a loss in the multicast
forwarding state on line cards under scaled conditions occurs.
  Conditions: This issue is observed when either of the following conditions is met:
  - The router is booted.
  - A high CPU load causes IPC timeout errors. The issue occurs on line cards during recovery from
an IPC error in the MRIB channel.
  Workaroud: There is no workaround. A line card reload might resolve the issue.
Open Caveats—Cisco IOS XE Release 3.1.3S

The following are the open caveats in Cisco IOS XE Release 3.1.3S:

- **CSCsk80075**
  
  Symptom: On a router with the SSO High Availability mode enabled, when the **no interface** multilink command is used to remove a multilink interface from the configuration, the standby RP may automatically reload.
  
  Conditions: This issue is observed when the multilink interface is active and the **shutdown** and **no interface multilink** commands are run in quick succession on the multilink interface.
  
  Workaround: After running the **shutdown** command, wait for a few seconds before running the **no interface multilink** command.

- **CSCtd08709**
  
  Symptom: When an LTS is restricted, CAC calls are not terminated through another LTS.
  
  Conditions: This issue is observed when an LTS is restricted.
  
  Workaround: Do not restrict CAC on the LTS.

- **CSCtd87072**
  
  Symptom: The router reboots when the tunnel mode is changed in scaled IPSec sessions.
  
  Conditions: This issue is observed when the tunnel mode is changed in scaled IPSec sessions.
  
  Workaround: There is no workaround.

- **CSCtf39056**
  
  Symptom: On a router running Cisco IOS 12.2(33)XND, RRI routes are not deleted automatically after the SA is cleared.
  
  Conditions: This issue is observed on a router running Cisco IOS 12.2(33)XND.
  
  Workaround: There is no workaround.

- **CSCtf54919**
  
  Symptom: The router crashes and CPU hog messages are displayed.
  
  Conditions: This issue is observed when the virtual access interface is shut down.
  
  Workaround: Apply one of the following workarounds:
  - When you remove an access list, remove the corresponding distribute list configuration.
  - Do not use the same access list name for both IPv4 and IPv6.

- **CSCtf71673**
  
  Symptom: A PRE crash occurs due to memory corruption with block overrun.
  
  Conditions: This issue is observed during PTA and L2TP access.
  
  Workaround: There is no workaround.

- **CSCtj46496**
  
  Symptom: When multiple physical OIR of the RP and ESP are performed at the same time, the RP might experience keepalive packet loss and then crash. Traffic issues might also be observed before the RP crashes.
  
  Conditions: This issue is observed when multiple physical OIR of the RP and ESP are performed at the same time. Note that this issue does not occur when a soft OIR is performed.
Workaround: There is no workaround.

- **CSCtj94121**
  Symptom: The RADIUS extended process leaks memory.
  Conditions: This issue is observed if the LNS is configured and the RADIUS extended process is in use.
  Workaround: There is no workaround.

- **CSCtj96760**
  Symptom: Unable to ping all bundles with **dlfi over atm in scaled configs in cwpa2**.
  Conditions: This issue is observed when more than 250 VT are created.
  Workaround: There is no workaround.

- **CSCtk05142**
  Symptom: Slow speed and increased latency is observed on the data path.
  Conditions: This issue is observed when a zone-based firewall is configured and a single high-volume flow is directed at the router when the firewall is enabled.
  Workaround: There is no workaround.

- **CSCtk76228**
  Symptom: When the **hw-module slot f0 reload** command is used during an FP switchover, the following error message is displayed:

```
%CPPOSLIB-3-ERROR.Notify: F0: cpp_cp: cpp_cp encountered an error
```
  Conditions: This issue is observed with the scaling configuration when there are a large number (for example, 8000 or more) of virtual circuits.
  Workaround: There is no workaround.

- **CSCtl09030**
  Symptom: The router crashes during the ARP input process.
  Conditions: This issue is observed when all of the following conditions exist at the same time:
  - The router is configured with the DHCP pool to function as the server for some clients and as the relay for other clients.
  - The DHCP database agent is enabled.
  - The ISG in-band IP session initiator is configured.
  - An ARP request is received from a client whose lease has expired.
  Workaround: There is no workaround.

- **CSCtl70143**
  Symptom: At times, the LAC does not forward the **PPP CHAP-SUCCESS** message from the LNS to the client.
  Conditions: This issue is observed when T1(PRI) is used between the LAC and the client.
  Workaround: There is no workaround.

- **CSCtl70677**
  Symptom: The FMAP FP crashes when the following command is run:
show platform hardware qfp active infrastructure shared-memory process forwarding-manager

Conditions: This issue is observed when the command mentioned in the Symptom description is run.
Workaround: There is no workaround.

- CSCtn11144
  Symptom: A QFP crash occurs.
  Conditions: This issue is observed when features such as MLP, VFR, and fragmentation and reassembly are used.
  Workaround: There is no workaround.

- CSCtn15317
  Symptom: Traffic on the MPLS VPN is dropped. In the LFIB entry on a P router, there is an instruction to tag all packets that are destined for the PE router instead of a POP instruction that is expected on a directly connected P router.
  Conditions: This issue is observed when all the following conditions exist at the same time:
  - The IS-IS protocol is running as IGP on MPLS infrastructure.
  - The IS-IS protocol on the PE router is summarizing the network that includes the BGP VPNv4 update source.
  - The P router is running an MFI-based image.
  Workaround: Apply one of the following workarounds:
  - Remove the summary address command in IS-IS on the PE.
  - Change the BGP update source.

- CSCtn19444
  Symptom: mLACP member links may be bundled on an isolated PoA with a core failure. This results in both PoAs becoming active.
  Conditions: This issue is observed while running mLACP and the ICRM connection between the PoAs is lost.
  Workaround: Set up shared control by configuring `lacp max-bundle` on the dual-homed device (DHD) if the device supports it. This prevents the DHD from bundling the member links to both PoAs at the same time.

- CSCtn25290
  Symptom: If the router is configured as a 6rd CE with `tunnel 6rd br` set, it cannot communicate with other CEs.
  Conditions: This issue is observed when the router is configured as a 6rd CE with `tunnel 6rd br` set.
  Workaround: There is no workaround.

- CSCtn38996
  Symptom: MVPN traffic is lost even when the peer is reachable using a TE Tunnel and an interface flap is performed so that the secondary path can be selected but the multicast route does not contain a native path using the physical interface.
  Conditions: This issue is observed when `mpls traffic-eng multicast-intact` is configured under OSPF.
  Workaround: Run the `clear ip ospf process` command on the core router.
• CSCtn43795
Symptom: A coredump may occur in the CPP client.
Conditions: This issue is observed when a CEF object is reparented and the previous parent is requested to delete itself. The delete operation of the parent might be carried out before the modify operation of the child is completed.
Workaround: To avoid the reparenting operation, do not use the `copy config` command.

• CSCtn44347
Symptom: The FP40 crashes.
Conditions: This issue is observed while configuring the route map on the router.
Workaround: There is no workaround.

• CSCtn48009
Symptom: The ESP crashes periodically, and the `%CPPOSLIB-3-ERROR_NOTIFY: F0` error message is displayed.
Conditions: There are no specific conditions under which this issue is observed.
Workaround: There is no workaround.

• CSCtn52207
Symptom: After an SSO, the MIB reports some extra instances. No messages are displayed on the console for these extra instances.
Conditions: This issue is observed after an SSO is performed.
Workaround: There is no workaround.

• CSCtn54703
Symptom: The shape rate limit is exceeded for priority traffic.
Conditions: This issue is observed when the same three-level service policy is configured on both a 10-Gigabit Ethernet and a 1-Gigabit Ethernet interface. When this happens, at times, the parent shape rate is not applied while sending priority traffic.
Workaround: Use a different service policy on each interface. In addition, ensure that the parent shape rate set for the two interfaces is not the same.

• CSCtn57731
Symptom: The ESP is automatically reloaded while removing the tunnel interface configuration.
Conditions: This issue is observed when the router functions as an IPSec termination and aggregation router for DMVPN hub deployment and when IVRF is not equal to FVRF.
Workaround: There is no workaround.

• CSCto03123
Symptoms:
1. A slow memory leak is observed on the `cman_fp` process on an FP and the `cmcc` process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
2. Additional memory leak can occur when frequent sensor value changes take place.
Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.
Workaround: There is no workaround.
PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- **CSCto21732**
  Symptom: When the Cisco ASR 1006 Router or Cisco ASR 1013 Router is started, the standby console does not show the `stby` extension in the host name.
  Conditions: This issue is observed when the Cisco ASR 1006 Router or Cisco ASR 1013 Router is booted with hardware redundancy with an RP2 advantereprise image (for example, asr1000rp2-adventerprise.03.01.03.S.150-1.S3.bin).
  Workaround: Use the `hostname` command to change the host name.

**Resolved Caveats—Cisco IOS XE Release 3.1.3S**

The following are the resolved caveats in Cisco IOS XE Release 3.1.3S:

- **CSCsl18054**
  Symptom: A local user created with a one-time keyword is automatically removed after failed login attempts. The expected behavior is that the one-time user should be removed after the first successful login, not after failed login attempts.
  Conditions: This issue is observed on a router running Cisco IOS Release 12.4.
  Workaround: There is no workaround.

- **CSCsy61302**
  Symptom: Chunk header corruption occurs, and the router crashes. The `BADMAGIC` error message is displayed for a chunk that is either free or in use.
  Conditions: This issue is observed when the following SNMP commands are configured:

    ```
    snmp-server community public ro
    snmp-server packetsize 17940
    ```

  Workaround: Do not set the packet size to a value greater than 2048.

- **CSCtd59027**
  Symptom: The router crashes due to a bus error.
  Conditions: This issue is observed when crypto is configured and running on the router. The issue may be linked to EzVPN.
  Workaround: There is no workaround.

- **CSCtd72318**
  Symptom: The Cisco ASR 1004 Router crashes at `__be_dhcpc_for_us`.
  Conditions: This issue is observed on a router running Cisco IOS Release 12.2(33)XNC2. The issue may be associated with DHCP configuration.
  Workaround: There is no workaround.
- **CSCte36327**
  Symptom: On the Cisco ASR 1002 Router, the standby RP is automatically rebooted at startup.
  Conditions: This issue is observed on the Cisco ASR 1002 Router.
  Workaround: There is no workaround.

- **CSCtf11309**
  Symptom: If the MFR interface has a policy map attached to it, the interface flaps when it is shut down and restarted.
  Conditions: This issue is observed when the MFR interface has a policy map attached to it.
  Workaround: There is no workaround.

- **CSCtf23298**
  Symptom: CPU usage is high when a TACACS server is configured with a single connection.
  Conditions: This issue is observed when the TACACS server is configured with a single connection.
  Workaround: Remove the single connection option.

- **CSCtf72328**
  Symptom: BFD IPv4 Static does not fully support the Admin Down state.
  Conditions: This issue is observed when the static route is deleted from the BFD neighbor.
  Workaround: Shut down and then restart the interface on which the BFD session is configured.

- **CSCtf83711**
  Symptom: A memory leak occurs after PPPoE sessions are tested.
  Conditions: This issue is observed after PPPoE sessions are tested.
  Workaround: There is no workaround.

- **CSCtf90182**
  Symptom: When a subinterface based PW (EoMPLS) is configured on SIP400, an SSO causes a traffic drop of 80 seconds. The VC on the peer router does not come up quickly. It goes to the Down state and then comes back up after 80 seconds.
  Conditions: This issue is observed during an SSO, when both LDP GR and OSPF NSF AWARE are configured.
  Workaround: Configure a longer hello holdtime when you run the following command:
  ```bash
  mpls ldp discovery hello holdtime holdtime_value
  ```

- **CSCtg59328**
  Symptom: When IPCP renegotiates for an existing PPPoE session, the new IPv4 address is not synchronized with the standby RP.
  Conditions: This issue is observed after the following steps are performed:
  1. Open a PPPoE session, and ensure that it is synchronized with the standby RP.
  2. From the PPPoE client, run the `no ip address` command followed by the `ip address negotiated` command under the virtual template interface.
  When the `no ip address` command is run, the session first switches to the Down state on both the active and standby RPs. The `ip address negotiated` command then triggers IPCP renegotiation, and the session switches to the Active state. However, on the standby RP, the session remains in the Down state and the new IP address is not synchronized.
Caveats in Cisco IOS XE 3.1S Releases

Workaround: There is no workaround.

- **CSCtg78106**
  
  Symptom: Even when SNMP is not configured on the router, the router shows SNMP ports as open or there are responses to SNMP requests.

  Conditions: This issue is observed when a specific set of configuration events are performed. To check whether the router is affected by this issue, run the `show ip sockets` or `show control-plane host open-ports` command. If the output of the command shows that the UDP 161 and UDP 162 SNMP ports are open and listening, run the `show running-config | include snmp` command. If this command does not return any output, it is confirmed that the router is affected by this issue.

  Workaround: Close the ports by performing the following steps:
  1. Configure an SNMP community. For example:
      ```
      snmp-server community workaround
      ```
  2. Use the `show snmp community` command to display the names of existing SNMP communities.
  3. Remove each SNMP community name by running the following command:
      ```
      no snmp-server community "community_name"
      ```
  4. Shut down the SNMP agent by running the following command:
      ```
      no snmp-server
      ```

- **CSCth03022**
  
  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.


- **CSCth14305**
  
  Symptom: If a bandwidth statement is configured on a multilink bundle interface and if the link members flap, changes in bandwidth are not handled correctly. This causes issues in QoS and BQS.

  Conditions: This issue is observed when a bandwidth statement is configured on a multilink bundle interface.

  Workaround: There is no workaround.

- **CSCth25634**
  
  Symptom: When logging in, a user is prompted for a password two times.

  Conditions: This issue is observed when login authentication has the line password configured as the fallback and the RADIUS password as the primary.

  Workaround: To change the login authentication to fall back to the enable password that is configured on the UUT, use a command similar to the following command:

  ```
  enable password keyword aaa authentication login default group radius enable
  ```

- **CSCth37580**
Symptom: A dampening route is present even after the BGP dampening configuration is removed.
Conditions: This issue is observed when the following sequence of events takes place:
1. DUT connects to RTRA with eBGP VPNv4.
2. An eBGP VPNv4 peer session is established and DUT.
3. DUT has the VRF (that is, the same RD) as the route advertised by RTRA.
In this scenario, when DUT learns the route, it imports the same RD and the topology of the network is changed from VPNv4 to VRF.
Workaround: There is no workaround.

- CSCth45731
Symptom: PPPoE sessions are partially synchronized with the standby RP. Later, these sessions are not cleaned up.
Conditions: This issue is observed when IPCP is renegotiated and then terminated before full session synchronization is performed for the PPPoE session that is starting.
Workaround: There is no workaround.

- CSCth45774
Symptom: The router crashes when the no ip policy routemap command is run on multiple interfaces.
Conditions: This issue is observed when the route map does not exist.
Workaround: Remove the policy configuration before removing the route map.

- CSCth66177
Symptom: If the standby PRE crashes, the active PRE also crashes.
Conditions: This issue is observed when the standby PRE crashes due to memory parity error. The standby PRE crash triggers an active PRE crash due to bus error.
Workaround: There is no workaround.

- CSCth69364
Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.
Cisco has released free software updates that address this vulnerability.

- CSCti48504
Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.
Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

- CSCti18615
Symptom: Reloading a router with multicast forwarding configured may result in the standby RP getting out of synchronization with the active RP. When this happens, the A and F flags are not included in the multicast forwarding base entries.

Conditions: This issue is observed when multicast forwarding is operational and configured in the startup-config file, the router is in High-Availability-mode SSO, and the router is reloaded from the RP.

Workaround: Shutting down and restarting the affected interfaces may fix the issue.

- CSCti34396
  Symptom: The router distributes an unreachable nexthop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.
  Conditions: This issue is observed when next-hop-unchanged allpaths is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is unreachable.
  Workaround: Configure a route map to rewrite routes so that the tunnel endpoint is an address that is reachable from both inside and outside the VRF.

- CSCti61949
  Symptom: The router is automatically reloaded, and the following error messages are displayed:
  ```
  SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header
  chunk name is BGP (3) update
  ```
  Conditions: This issue is observed while receiving BGP updates from a speaker for a multicast-enabled VRF.
  Workaround: Disable multicast routing on VRFs participating in BGP. Alternatively, reduce the number of extended communities that used as route-target export.

- CSCti85446
  Symptom: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.
  Conditions: This issue is observed when the nexthop static route is configured with a permanent keyword.
  Workaround: Delete all static routes that pass through the affected nexthop, and then add them again.

- CSCti98931
  Symptom: Some sessions may be lost after an L2TP switchover.
  Conditions: This issue is observed after an L2TP switchover.
  Workaround: There is no workaround.

- CSCti08533
  Symptom: QoS classification fails on egress PE if the route is learned through BGP.
  Conditions: This issue is observed when there are redundant paths to the CPE.
  Workaround: Use only one path between PE and CPE.

- CSCti17545
  Symptom: After a switchover, the restarting speaker sends TCP-FIN to the receiving speaker, when receiving speaker tries to establish (Active open). This may cause packets to be dropped.
  Conditions: This issue is observed when a large number of BGP peers are set up on different interfaces.
  Workaround: Configure the receiving speaker to accept passive connections.
- **CSCtj24453**
  
  **Symptom:** A traceback message is displayed when the `clear ip bgp *` command is run.
  
  **Conditions:** This issue is observed when there are a large number of routes and route map cache entries.
  
  **Workaround:** Run the `no bgp route-map-cache` command to ensure that route map results are not cached.

- **CSCtj30462**
  
  **Symptom:** Details of subscribers are not correct.
  
  **Conditions:** This issue is observed under any one of the following conditions:
  - High system usage.
  - Incorrect download of a previous service.
  - The same subscriber is present in two different PPPoE sessions.
  
  **Workaround:** There is no workaround.

- **CSCtj48629**
  
  **Symptom:** Although `ppp multilink load-threshold 3` either is set, member links are not added by inbound heavy traffic on the PRI of the HWIC-1CE1T1-PRI.
  
  **Conditions:** This issue is observed on a router running Cisco IOS Release 15.0(1)M2.
  
  **Workaround:** There is no workaround.

- **CSCtj58943**
  
  **Symptom:** When the `encapsulation dot1q 1381` command is used, the standby RP reloads due to line-by-line synchronization failure.
  
  **Conditions:** This issue is observed when a configuration command is run under a subinterface mode.
  
  **Workaround:** There is no workaround.

- **CSCtj61748**
  
  **Symptom:** Service activation may fail.
  
  **Conditions:** This issue is observed when there are multiple services in the session authentication and authorization response.
  
  **Workaround:** Remove the Service Group and Service Type fields from the service definitions.

- **CSCtj65553**
  
  **Symptom:** A static route that is installed in the default table is automatically removed.
  
  **Conditions:** This issue is observed after a RP to line card to RP transition.
  
  **Workaround:** Add the missing static route.

- **CSCtj77004**
  
  **Symptom:** While PPPoE sessions are getting established, the archive log configuration size impacts CPU utilization. In addition, only some configuration lines from the virtual template are copied to the archive. The remaining configuration files are not copied.
  
  **Conditions:** This issue is observed when `archive log config` is configured.
  
  **Workaround:** There is no workaround.

- **CSCtj82292**
  
  **Symptom:** The EIGRP summary address with AD 255 is sent to a peer.
Conditions: This issue is observed when the summary address is advertised as follows:

```
ip summary-address eigrp AS# x.x.x.x y.y.y.y 255
```

Workaround: There is no workaround.

- CSCtj87180
  Symptom: An LAC router running VPDN may crash when it receives an invalid redirect from its peer. The **SSS Manager Disconnected Session CDN** error message is displayed.
  Conditions: This issue is observed when the LAC router receives the following incorrect message from its multihop peer:

```
Error code(9): Try another directed and Optional msg: SSS Manager disconnected session <<<< INVALID
```

Workaround: There is no workaround.

- CSCtj89941
  Symptom: The router crashes when the `clear crypto session` command is used on an EzVPN client.
  Conditions: This issue is observed when the `clear crypto session` command is used on an EzVPN client.
  Workaround: There is no workaround.

- CSCtj94141
  Symptom: A memory leak occurs.
  Conditions: This symptom is observed while creating an SLA MPLS probe through SNMP.
  Workaround: Use the CLI to configure the SLA MPLS operation.

- CSCtj94555
  Symptom: After a router is reloaded, it is not able to re-register with the KS.
  Conditions: This issue is observed on a router running Cisco IOS 15.0(1)S1.
  Workaround: Run the `clear crypto gdoi` command.

- CSCtj96915
  Symptom: The LNS router stops responding at the interrupt level.
  Conditions: There are no specific conditions under which this issue is observed.
  Workaround: There is no workaround.

- CSCtk00976
  Symptom: The file descriptor reaches its maximum threshold limit. The **File table overflow** error message is displayed, and you cannot save the configuration or perform a file-system-related operation.
  Conditions: This issue is observed when the `dir/recursive <>` command is run multiple times by using the ANA tool.
  Workaround: Do not run the `dir/recursive <>` command if leaks are detected. In addition, if the command is running through ANA server polling, disable it.

- CSCtk02647
  Symptom: On an LNS router configured for L2TP aggregation, per-user ACLs downloaded through RADIUS may cause PPP negotiation failures (that is, IPCP may get blocked).
Conditions: This issue is observed when an LNS multilink is configured and negotiated for PPP/L2TP sessions and per-user ACL is downloaded for PPP users through RADIUS.

Workaround: There is no workaround.

- CSCtk12252
  Symptom: After the router is reloaded, a Priority 1, valid SONET controller network clock source is not selected as the active clock source. Instead, the clock remains in the FREERUN state.
  Conditions: This issue is observed after the router is reloaded, when there is a Priority 2 network clock source in the Valid But Not Present state.
  Workaround: Shut down and restart the near-end Priority 1 clock source SONET controller.

- CSCtk12608
  Symptom: Route watch does not notify the client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.
  Conditions: This issue is observed when a RIB resolution loop changes.
  Workaround: Use static routes tied to specific interfaces instead of using floating static routes.

- CSCtk12708
  Symptom: The router crashes when the holdover clock source is deleted.
  Conditions: This issue is observed when the holdover clock source is deleted.
  Workaround: There is no workaround.

- CSCtk30807
  Symptom: A router that acts as a DHCP relay or server crashes when the DHCP service is stopped and then started.
  Conditions: This issue is observed when the router is also configured as the ISG.
  Workaround: There is no workaround.

- CSCtk35953
  Symptom: Dampening information is not removed even when the dampening configuration is removed in VPNv4 AF.
  Conditions: This issue is observed when DUT has an eBGP-VPNv4 session with a peer and a same-RD import occurs on the DUT for the route learned from the VPNv4 peer.
  Workaround: Perform a hard reset of the session to remove the dampening information.

- CSCtk36582
  Symptom: The Acct-On and Acct-Off signals from the AZR clears all the sessions in the client pool.
  Conditions: This issue is observed in scenarios similar to the following sample scenario:
  There are two AZRs, 192.168.100.1 and 192.168.100.2. The client in the ISG is configured under the RADIUS proxy as follows:
  client 192.168.0.0 255.255.0.0
  When Acct-on and Acct-off signals are received from one of the clients, sessions on both clients are cleared.
  Workaround: Configure clients one at a time instead of configuring the entire pool.

- CSCtk47891
  Symptom: If FRR is configured, traffic may be lost when the LC is reset.
Conditions: This issue is observed when FRR is configured and is in the Active state when the LC is reset.
Workaround: There is no workaround.

- CSCtk53463
  Symptom: While running the `shape average cir_value bc_value` command, `bc_value` is limited to 4 milliseconds times `cir_value`. Here, 4 milliseconds is the minimum interval between bursts. However, the ES LC can support intervals that are smaller than 4 milliseconds. This is not the expected behavior for the ES LC.
  Conditions: There are no specific conditions under which this issue is observed.
  Workaround: There is no workaround.

- CSCtk67658
  Symptom: While running the `shape average cir_value bc_value` command, `bc_value` is limited to 4 milliseconds times `cir_value`. Here, 4 milliseconds is the minimum interval between bursts. However, the ES LC can support intervals that are smaller than 4 milliseconds. This is not the expected behavior for the ES LC.
  Conditions: There are no specific conditions under which this issue is observed.
  Workaround: There is no workaround.

- CSCtk67768
  Symptom: The RP crashes during the DHCPD Receive process.
  Conditions: This issue is observed when a DHCP server is configured.
  Workaround: There is no workaround.

- CSCtk74970
  Symptom: A tunnel that is announced by the TE autoroute is not installed in the routing table.
  Conditions: This issue is observed when you first configure and remove one hop and LDP from the TE, and then configure one hop on the TE (without LDP).
  Workaround: Run the `no ip routing protocol purge interface` command.

- CSCtk75389
  Symptom: The PFR fallback interface does not stay in-policy.
  Conditions: The issue is observed when an ATM interface is used.
  Workaround: There is no workaround.

- CSCtl00127
  Symptom: The output of the `show ip int` command does not indicate whether the `ip security ignore-cipso` option is configured and operational.
  Conditions: There are no specific conditions under which this issue is observed.
  Workaround: There is no workaround.

- CSCtl04285
  Symptom: The BGP route reflector does not advertise new IPv4 MDT routes to PEs.
  Conditions: This issue is observed after a BGP session flap or while provisioning a new session.
  Workaround: Run the `clear ip bgp *` command.

- CSCtl08014
  Symptom: The router crashes and memory corruption symptoms are observed.
Caveats in Cisco IOS XE 3.1S Releases

Conditions: This issue is observed when SSO or OIR is performed while MLP sessions are getting initiated.

Workaround: There is no workaround.

- CSCtl08601
  Symptom: When the DHCP pool is removed, the console stops responding.
  Conditions: This issue is observed when the `no service dhcp` command is run before the DHCP pool is removed.
  Workaround: There is no workaround.

- CSCtl21884
  Symptom: When autosummary is enabled under the BGP process, a BGP withdraw update is not sent even though the static route becomes unavailable.
  Conditions: This issue is observed when autosummary is enabled under the BGP process and a static route is brought into the BGP table by running the `network` command.
  Workaround: Under the BGP process, run the `clear ip bgp *` command or disable autosummary.

- CSCtl42358
  Symptom: The router crashes after the `no atm sonet overhead j1` command is run on an ATM interface.
  Conditions: This issue is observed after the `no atm sonet overhead j1` command is run on an ATM interface.
  Workaround: There is no workaround.

- CSCtl54033
  Symptom: After a sub-LSP is pruned or torn down, resignaling sub-LSPs for P2MP TE tunnels may require up to 10 seconds.
  Conditions: This issue is observed when a P2MP TE tunnel is configured to request FRR protection but no backup tunnel is available at the failure point to protect the sub-LSP.
  Workaround: Configure FRR backup tunnels at each node to provide link protection for P2MP TE tunnels.

- CSCtl67195
  Symptom: The following BGP debug commands cannot be used:
  ```
  debug ip bgp vpnv4 unicast
  debug ip bgp vpnv6 unicast
  debug ip bgp ipv6 unicast
  ```
  Conditions: There are no specific conditions under which this issue is observed.
  Workaround: There is no workaround.

- CSCtl83053
  Symptom: The shaper rate cannot be changed with ANCP Port Up messages.
  Conditions: This issue is observed when QoS and ANCP are enabled.
  Workaround: There is no workaround.

- CSCtl83736
Symptom: Each V4 session setup leaks approximately 100 bytes. Similarly, each V6 session setup leaks approximately 112 bytes.
Conditions: This issue is observed on IP sessions.
Workaround: There is no workaround.

- CSCtl88066
  Symptom: The router is automatically reloaded.
  Conditions: This issue is observed when BGP is configured and one of the following commands is run:
  `show ip bgp all attr nexthop`
  `show ip bgp all attr nexthop rib-filter`
  Workaround: Do not run either of these commands with the `all` keyword. Instead, run the address-family-specific version of the command for the address family.

- CSCtn01832
  Symptom: The router crashes when the following command is run:
  `config check syntax route-map hello match local-preference no match local-preference`
  Conditions: This issue is observed when the command mentioned in the Symptom description is run.
  Workaround: There is no workaround.

- CSCtn03930
  Symptom: A system error may be logged.
  Conditions: This issue is observed when RP switchover takes place while traffic is running on a router that functions as an IPSec termination and aggregation router.
  Workaround: There is no workaround.

- CSCto88686
  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.
  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

Open Caveats—Cisco IOS XE Release 3.1.2S

This section documents possible unexpected behavior by Cisco IOS XE Release 3.1.2S

- CSCsa79984
  When using the line subcommand `login`, it may be possible for a vty to get into a state where the user will not be able to log in to the IOS router. The user will be presented with password followed immediately by “Bad passwords”.
  The line in this state can be seen with the exec command `show line <line number>`. In the “Status line”, if ‘Ctrl-c Enabled’ appears, then you may see this problem on that line.
Workaround: To clear this condition follow these sequence of steps:
1. First remove the login from the line.
2. Telnet into the router on the line which is in this state. From enable mode, run the command `setup`.
3. When prompted with “Continue with configuration dialog” type no.
4. Add the login back to the vty line.

- CSCtf84408
  Burst remove TP might cause iosd Segmentation fault(11) at Tunnel Security process.
  This condition is observed when using interface range command to remove TP from tunnel interface.
  Workaround: There is no workaround.

- CSCth11310
  IP-subscriber sessions stop forwarding traffic after RADIUS proxy resets them. The session does not appear to get any traffic, and drops may be observed when the following command is used:
  `show platform hardware qfp active statistics drop`
  This behavior may occur on ASR 1000 Router Series, with routed IP-subscriber sessions that are reset and converted to RADIUS proxy sessions.
  Workaround: There is no workaround.

- CSCth12830
  CE to CE ping fails on SSO switchover with L2TPv3 configuration on ATM interface.
  This condition has been observed when CE to CE ping fails on SSO switchover with L2TPv3 configuration on ATM interface with VP mode.
  Workaround: Is issue the `clear xconnect all` command.

- CSCth22250
  On 2RU-F and ESP-5 when bringing up translations at higher rate, all sessions cannot be established with high setup rate.
  Workaround: Lower the setup rate.

- CSCth74294
  On the ASR 1000 Router “stop” accounting message is seen on the router console for Acct-Input-Octets missing field:
  Acct-Output-Octets, Acct-Input-Packets, Acct-Output-Packets
  This condition is observed in DVTI- EzVPN topology during session tear down while the EzVPN server sends out accounting information.
  Workaround: There is no workaround.

- CSCti40325
  RADIUS retransmit timeout happens (roughly) at half the timeout configured by the `radius-server timeout` command. For example, for the default timeout value of 5 seconds, timeout happens at 2 to 3 seconds. For higher values, for example 20, timeout happens at around 10 seconds.
  This symptom is seen when the RADIUS server is used for AAA.
  Workaround: There is no workaround.
• CSCtj05670
  When doing SSO with scaled mLDP configuration, path set for some of the VRFs are not configured.
  This issue only occurs when configuring mLDP on 100 VRFs with 100 receivers.
  Workaround: There is no workaround.

• CSCtj15181
  SMAND may not initiate when issuing `show policy-map type inspect zone-pair session` command.
  Workaround: Use HSL for retrieving `zone-pair` information.

• CSCtj16111
  ESP may not initiate on the Cisco ASR 1000 Router. This condition is seen when the router is configured as an ISG gateway, and has periodic L4 redirection configured for user sessions.
  Workaround: If the periodic redirection is not configured then the crash is avoided.

• CSCtj23259
  When the ASR 1000 Router acts as a PE and has scaled configs for L2TPv3 feature combination with EoMPLS and ATMoMPLS with 2000 pseudowires. A CC failure is observed when initiating CC OIR.
  This condition may occur when initiating CC OIR and the CC failure is observed. This may only happen when SIP has been configured with SPA-1XCHOC12/DS0's and SPA-2XOC3-POSs. This condition is not observed with any other SPAs.
  Workaround: There is no workaround.

• CSCtj31267
  IPv4 Multicast NAT traffic might create dynamic NAT 1 to 1 binding even when the traffic flow is not into out, or out to in on the ASR 1000 Router.
  Workaround: There is no workaround.

• CSCtj62999
  PPP sessions are not able to activate on the ASR 1000 Series Router.
  This condition is observed when PBR is configured under Virtual-template interface.
  Workaround: There is no workaround.

• CSCtj73536
  Traffic may stop when forwarding over to PPP Users, after PPP Users have been terminated on the Cisco ASR 1000 Router with L2TP Tunnel configured.
  This condition is observed when flapping occurs on the virtual-access interface, several times.
  Workaround: There is no workaround.

• CSCtj74404
  PEM status is not updating correctly even though one of the redundant PEMs are switched off (PEM status is still ok).
  This condition is observed when initiating the following:
  - After power cycle, or reload has occurred. If PEM status does not appear right after bootup, you may not see it's next power cycle
  - When using Cisco IOS XE 3.1.xS
Caveats in Cisco IOS XE 3.1S Releases

Workaround: Reload or power cycle the box again.

- CSCtj80468
  ASR 1000 Series Router ESP-20 may experience failures during high sustainable churning, per-subscriber and Zone-based Firewall Stateful sessions after throughput has high PPP subscriber sessions churning.
  This condition is observed when the ASR 1000 Series Router is configured as an LNS, has ~15000 PPP subscribers in the Zone-based firewall with heavy stateful traffic, ~15000 PPP subscriber not having their traffic inspected, and there are numerous other subscriber churning activities. This has been observed in an MPLS environment, as well. If Aggregate traffic is between 7-10Gb's.
  Workaround: Is to back off traffic load and churn.

- CSCtj88724
  Standby ESP fails to activate and Traceback is thrown on the console after unconfiguring the interface while Broadband sessions are still up.
  This condition is observed when unconfiguring the Interface while Broadband sessions are still up on the router causing Standby ESP fails to activate and traceback is thrown on the console. In addition this failure, or traceback is not affecting the basic functionality of the router.
  Workaround: Stand by ESP failure is not always seen and since active ESP is always up, there is no interruption for service.

- CSCtj94131
  Only on the ASR 1002 Router the parse configuration time (is 5 seconds) may take too long.
  Workaround: There is no workaround.

- CSCto03123
  Symptoms:
  1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
  2. Additional memory leak can occur when frequent sensor value changes take place.
  Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.
  Workaround: There is no workaround.
  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.
  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.
  Additional information on Cisco's security vulnerability policy can be found at the following URL:

Resolved Caveats—Cisco IOS XE Release 3.1.2S

All the caveats listed in this section are resolved in Cisco IOS XE Release 3.1.2S

- CSCsj78195
  Cisco IOS NAT CLI allows route-maps to be configured when defining static network translations.
Due to the current implementation of NAT and route-maps the use of route-maps with a static network translation is currently not supported. Therefore the CLI should block this configuration.

Workaround: There is no workaround.

- **CSCsm98756**
  
  CPU utilization peaks at 99% for a sustained period and various control plane functions such as SBC call setup may not function as expected. The symptom is observed with a large scale configuration (thousands of VLANs) and when performing the `show run | inc ipv6 route` command.

  Workaround: There is no workaround.

- **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.

  Workaround: There are no known workarounds.

- **CSCsq70140**
  
  The following error messages may seen may be seen on Cisco ASR 1002 and Cisco ASR 1004:

  No memory available: Update of NVRAM config failed!

  This happens more frequently when user are saving a very big configuration such as one with 16K interfaces on a ASR 1002 or ASR 1004. This problem is not seen on Cisco ASR 1006.

  Workaround: There is no workaround.

- **CSCsq73935**
  
  Invalid instance “0” is getting populated for tabular objects in `dsx3ConfigTable`. This issue is observed when configuring sonet framing on 1xCHSTM1/OC3-SPA, after the mode is set to “ct3” or “ct3-e1” and the “0” instances gets populated for the tabular objects.

  Workaround: This instance may be seen, when configuring any channelization on top:

  ```
  controller sonet 0/3/0
  sts1-1
  mode ct3
  ```

  **Note** If the mode is set to “ct3” or “ct3-e1”, the “0” instances are not returned

- **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.

- **CSCsr50040**
  
  If you disable `aaa policy interface-config allow-subinterface` on the Cisco ASR 1000 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.

- **CSCsr87974**
When the online insertion and removal (OIR) of a SIP is performed on a Cisco ASR 1000 Router, traceback occurs at fibidb_configure_lc_ipfb. No functional impact is observed.

**Workaroud:** There are no known workarounds.

- **CSCsr90264**
  When Per-subscriber firewall PPoX calls may not initiate, **Zoning is currently not configured for interface Virtual-Access** logs might appear.

This condition is observed when Per-subscriber firewall is configured in a PPPoE environment. The involved virtual-template(s) contain a zone security statement placing the virtual-template in a zone. This zone is part of a valid zone-pair configuration and working service policy for that zone-pair. RADIUS authentication is used and the subject subscriber will download the same zone statement in their user profile as is described in the virtual-template to which this subscriber is being applied.

For example: `lcp:interface-config=zone-member security zone_name`.

The subscriber may not initiate its call attempt and router logs will include **Zoning is currently not configured for interface Virtual-Access**.

**Workaroud:** Use a different zone name belonging to a zone-pair with the same service policy as intended in the failing example above. Make sure `aaa policy interface-config allow-subinterface` is configured and not doing the analogous `lcp:interface-config=allow-subinterface=yes` via RADIUS in addition or concurrently.

**Further Problem Description:** If what otherwise looks to be a valid config, enable vtemplate debugging (cloning, error, and subinterface at a minimum). The `lcp:interface-config` provisions the session as if you’d type the commands through the parser. The parser may return error messages, when such messages are detected, SSS assumes in the config manager that something went wrong and that results in a disconnect:

```
*Aug 10 03:35:03.873: VT:Messages from (un)cloning Vi2.1:  
% Interface is already member of zone fw_low_zone *Aug 10 03:35:03.874: SSM CM: Query Lterm to L2TP switching, enabled  
And that results eventually in :  
*Aug 10 03:35:03.894: VT[Vi2.1]:Processing vaccess response, id 0x41D3D6C8, result clone error (4) *Aug 10 03:35:03.894: SSS MGR [uid:2]: Event feature-failed, state changed from installing-config to disconnecting-all  
```

This feature does not get reapplied, it throws an error message and that is when the session disconnects.

- **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.

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

- **CSCsv29870**
  RIP sends multiple request after doing `clear ip route *` and interface state transitions.

This condition is observed when RIP is configured and issuing `clear ip route *` afterwards RIP sends a multiple request for each interface instead of sending one request. This will cause the processing load on the request receiving side.

**Workaroud:** There is no workaround.

- **CSCsx13031**
The Route Processor (RP) on a Cisco ASR 1000 Series Router may reload unexpectedly shortly after switchover.

This condition is observed when the redundancy force-switchover command is executed immediately (within seconds) after the system reaches Stateful Switchover (SSO) mode.

Workaround: There are no known workarounds.

- **CSCsx56362**
  BGP selects paths which are not the oldest paths for multipath on a Cisco ASR 1000 Router. This causes BGP to unnecessarily flap from multipath to non-multipath as a result of route flaps.

  This condition has been observed when initiating the following:
  1. BGP is configured
  2. More than one equally-good route is available
  3. BGP is configured to use less than the maximum available number of multipaths

  Workaround: There is no workaround.

- **CSCsy31159**
  When the `show history all` command is executed on a Cisco ASR 1000 Series Router, the command does not immediately reflect all commands entered.

  Workaround: There are no known workarounds.

- **CSCsy49927**
  The IOSd restart is seen with crest proc frame that fetches the tcl shell for execution.

  This is seen with crest proc that helps in configuring a scale configuration.

  Workaround: There is no workaround.

- **CSCsy85400**
  The first VIA field in a Session Initiation Protocol (SIP) INVITE/BYE call is not getting properly translated by Network Address Translation (NAT). The NAT inside IP address is replaced by some invalid characters. Calls are NOT impacted due to this issue.

  This condition happens when no existing NAT translation for the session exists.

  Workaround: There are no known workarounds.

- **CSCsy88034**
  The “active” and “individual flow data” in the `show ip cache [verbose] flow` command output intermittently fails on a Cisco ASR 1000 Series Router. At times the “active” stat is zero, and at other times the individual flow data is missing.

  This problem occurs with very large configurations.

  Workaround: Reload the router.

- **CSCsz37418**
  There is no NHS entry on the HUB in SNMP tree.

  This condition is observed when the images are unable to initiate to create a Server entry on the HUB after some events.

  For example, the following events are seen:

  If the tunnel is configured after doing a `shut/no shut`, when the spoke has re-registered and verified by viewing the syslog messages the images are unable to initiate to create a Server entry on the HUB.
Workaround: There is no workaround.

- **CSCsz53438**
  On the Cisco ASR 1000 Series Router, if IP header compression is configured on the router, but not on the corresponding router, an unexpected reload of the embedded systems processor may occur. This condition may occur when IPHC is configured on the ASR 1000 Series Router, but not on the router to which it is directly connected to.
  Workaround: Is to enable IPHC on both routers.

- **CSCsz56462**
  When configuring cdp run it does not bring up cdp on the interfaces. This Conditions happens only if the default behavior of a platform is to have CDP disabled.
  Workaround: To enable CDP, include the cdp enable command in the configuration.

- **CSCsz56462**
  When configuring cdp run it does not bring up Cisco Discovery Protocol (CDP) on the interfaces. This conditions happens only if the default behavior of a platform is to have CDP disabled.
  Workaround: To enable CDP, include the cdp enable command in the configuration.

- **CSCsz82080**
  An Cisco ASR 1000 Router may not activate with ESP when an IPSec Tunnel is removed or modified.
  Workaround: When modifying or removing a tunnel interface remove the IPSec command first. After the change has been made IPSec can then be applied again.

- **CSCta31582**
  The netflow export command `ip flow-export version 9 bgp-nexthop` by itself has no effect meaning no BGP nexthop information is placed into the Netflow cache or records as a result of the bgp-nexthop token. If instead the commands `<CmdBold>` ip flow-export version 9 origin-as bgp-nexthop or `ip flow-export version 9 origin-as` are issued, then BGP nexthop information is included in all cases.
  This instance can occur on any ASR 1000 Router platform running the NetFlow feature.
  Workaround: The workaround is covered in the above description. If BGP Nexthop info is desired configure either `origin-as` or `peer-as` in the exporter command and this will cause BGP Nexthop information to appear in the cache and the export records.

- **CSCta43825**
  A CMTS walk of the ARP table causes high CPU usage.
  This symptom is also seen with an SNMP walk of the ARP table.
  Workaround: To prevent high CPU usage due to SNMP walk, implement SNMP view to prevent SNMP walk of the ARP table:
  ```
snmp-server view cutdown iso included
snmp-server view cutdown at excluded
snmp-server view cutdown ip.21 excluded
snmp-server community public view cutdown ro
snmp-server community private view cutdown rw
  ```

- **CSCta65347**
  There is no media after resuming the call on the ASR 1000 Router Series. Only in this instance the resume fails, when CCM/CME scenario's from h323 legcalls are used.
Workaround: There is no workaround.

- CSCta69213

When the Cisco ASR 1000 Series Router is configured for NHRP it may not activate due to a bus error.

This symptom is observed on a Cisco ASR 1000 Router configured for NHRP and DMVPN.

Workaround: There is no workaround

- CSCtb24959

The ASR 1000 Router may fail while clearing large number of rp mappings.

This instance can happen when the following has occurred:
1. The router has been configured for RP agent
2. and candidate there are a large number of RPs.
3. When initiating the clear ip pim rp-map command
4. a failure has been observed on the router.

Workaround: Is not to apply the clear ip pim rp-map command one after the other.

- CSCtb32892

Traceback has been logged %MFIB-3-DECAP_OCE_CREATION_FAILED: Decap OCE creation failed may be seen on the ASR 1000 Router Series console when loading the image or adding the RP with SSO.

In this condition, the tracebacks can be seen on reloading a Provider Edge router with mVPN configuration or adding the RP with SSO on the router.

Workaround: There is no workaround.

- CSCtb33587

NDB state Error Tracebacks on DMVPN spoke with NHO may be found on the ASR 1000 Router Series:

%IPRT-3-NDB_STATE_ERROR: NDB state error (NO NEXT HOPS UNEXPECTED)

This may cause temporary packet drops or forwarding to less specific routes.

The problem may occur, when using RIP or EIGRP and running NHRP and NHRP has installed NHO nexthops for the RIP/EIGRP route.

Workaround: Is to wait after the holddown timer expires, the problem will be cleared.

- CSCtb79598

When you configure a PVC ASR 1000 with QoS enabled, the QoS will not work as expected on the ASR 1000 Router Series.

The only happens, when you unconfigure ancp neighbor associated with the PVC before you delete the PVC on the ASR 1000 Router.

Workaround: There is no workaround.

- CSCtb84718

Output of show cli “sh crypto gdoi gm acl” does not correctly display as a COOP Key Server.

This has been observed, when COOP Key Servers has been configured on the GM.

Workaround: There is no workaround.

- CSCtc19914
The Embedded Services Processor (ESP) has been reloaded when configuring and unconfigure a large static RP addresses multiple times rapidly with mVRFs on the ASR 1000 Router Series.

This condition has been seen when using the following scripts:

1. Configuring large mVRFs on PE
2. Configuring large loopbacks on PE, one for each of the VRF
3. Configuring and unconfiguring large static RP addresses multiple times rapidly.

Workaround: There is no workaround.

- **CSCtc21042**
  Chassis-manager process on RP2 gets stuck and the ASR 1000 Router becomes unresponsive to user commands. All the FPs and CCs keep rebooting, with console logs showing repeated FP code downloads.

No particular scenario is known. This problem may caused by OBFL logging of messages on RP2.

Workaround: Is to disable onboard logging of messages on RPs as shown in this following example:

```
hw-module slot r0/r1 logging onboard disable
```

To verify that onboard logging has been disabled:
```
Router#sh logging onboard slot r0 status
Status: Disabled
```

**Note**

This command is not saved in the config so is not preserved across router reloads.

Workaround: There is no workaround.

- **CSCtc25791**
  A router may not activate when issuing `show` commands related to EIGRP and routing information while the EIGRP configuration is being removed.

This symptom is observed when EIGRP is configured when there are minimum of two users logged into the device issuing `show` commands.

Workaround: Do not issue `show` commands regarding EIGRP or routing while removing the EIGRP configuration.

- **CSCtc55049**
  The ASR 1000 Router may not initate and reload following a reboot or initial boot from a power-up. The embedded syslog manager (ESM) needs to be configured along with an ESM script present during an initial boot or reload. Also, redundant RP/FP appears to be the scenario that has the greatest likelihood of encountering the problem.

Workaround: There is no workaround. However, if the problem manifests, the subsequent rebooting is very likely to be successful. When stuck in a situation where crashes are repetitive, momentarily pull redundant RP until system stabilizes, and re-insert redundant RP.

- **CSCtc62440**
  On a Cisco ASR 1000 Router Series, the removal of subinterfaces may under certain conditions result in `MFIB_MRIB-3-FAILED_WIRE_FIND` error messages being generated on the Route Processor (RP).
There is no functional impact due to this issue. Workaround: There are no known workarounds.

- CSCtc72052
  The ASR 1000 Router is unable to configure Dynamic Nat Pool with prefix length 14 or less. This happens when Nat Pool is configured with a lower prefix lengths. This configuration is rejected on the ASR 1000 Router.
  Workaround: Is to create a Nat Pool with prefix length 14 or higher.

- CSCtc73525
  The ESP board on the ASR 1000 Router Series with ATM PVCs carrying broadband sessions does not accept further config. Traffic forwarding on existing features and session is not impacted, but additional config is rejected.
  This occurs when BB sessions over ATM PVCs are configured. With a high number of PVCs configured, and if all PVCs are attempted to be removed at once with the "rage" command, the ESP board may get into an error state that prevents additional config (such as bringing up new PVCs or sessions) from being accepted.
  Workaround: There is no workaround. However if problem manifests, a reload of the ESP is required to bring the system back to its normal state.

- CSCtd13999
  When an ASR 1000 Router is running IOS the router may pick an incorrect MSS when path-mtu is enabled. The incorrect MSS is lower than what the network path can support.
  This symptom is triggered when a transit router sends more than one ICMP-too-big messages.
  Workaround: There is no workaround.

- CSCtd14559
  L2TP-3-ILLEGAL tracebacks and PPPoX session mismatch between active and standby rps.
  This error condition is noticed, when rp switchover takes place during the time frame pppox sessions are coming up. In a rare condition, session mismatch was noticed when pppox sessions were coming up for the first time with no other events taking place.
  Workaround: There is no known workaround

- CSCtd21252
  Unified SBC crash has been seen on the ASR 1000 Router Series.
  This condition may occur, when configuring a large IPv6 media-address on the router.
  Workaround: There is no workaround.

- CSCtd32560
  During Cisco ASR 1002 or Cisco ASR 1004 ISSU upgrade from IOS XE 2.3.2 to IOS XE 2.5.0, a loss of QoS functionality can occur on some and all targets.
  Loss of QoS functionality has been observed right after RP upgrade and switchover while following Cisco ASR 1002 or Cisco ASR 1004 ISSU procedure. The QoS functionality does not recover on its own and only occurs on policies that are both hierarchical (at least 2-level) and contain policers. The condition can be identified by the following command:
  
  show platform hardware qfp active interface if-name <if_name> info | include QoS
  
  If there is no output returned from this command then there has likely been a QoS service disruption due to this problem.
Workaround: QoS functionality can be resumed on the interface by removing and re-attaching the QoS policy. Alternately, the problem can be avoided by upgrading to IOS XE 2.4.x first (including the ESP). The upgrade path would be IOS XE2.3.2 -> IOS XE 2.4.x -> IOS XE 2.5.x.

- **CSCte09945**
  When an Cisco ASR 1000 Router operates in the Unified SBC mode, after a hardware switch over using CLI `redundancy force-switchover`, during the old active RP is booting, issue CLI `no sbc`. Check failure error is observed in the RP console log.
  Workaround: No workaround until now.

- **CSCte14955**
  A Cisco ASR 1000 Series Aggregation Services router may experience an unexpected reload. The symptom may occur when multiple tunnel interfaces are configured with mpls bgp forwarding, if the tunnel interfaces are flapping.
  Workaround: Configure the eBGP sessions on interfaces other than tunnel interfaces.

- **CSCte17127**
  Calls are failing due to an invalid tls certificate or they may be completing when the certificate is invalid.
  This issue ties into how long the SBC keeps the tcp and tls connection up and also when the ASR 1000 Router does not revalidate the certificates for a deleted or newly added trust point tls peer. The same applies to the scenario where a certificate has to be replaced.
  Workaround: Set the tls idle timer to a value of 3 minutes to minimize the time that the tls peer. This will cause the ASR 1000 Router to revalidate the certificate. Another option is to use the `show tcp brief` command to find the peer connections and then use the `clear tcp brief tcb XXXXX` to clear the existing connections. This will cause the ASR 1000 Router to revalidate the peer.

- **CSCte61735**
  Memory leak has been seen when MQC is configured on the Cisco ASR 1000 Router. This can occur, when QoS has been configured on the router, in an ISG environment.
  For example the following conditions have been observed:

  ```
  interface ATM4/0.1 point-to-point
  no atm enable-ilmi-trap
  pvc 0/101
  class-vc crosshairs
  vbr-nrt 500 400 50
  dbs enable
  service-policy in DefaultIn
  service-policy out DefaultOut
 !
  vc-class atm crosshairs
  protocol ppp Virtual-Template1
  encapsulation aal5snap
  
  interface Virtual-Template1
  ip unnumbered Loopback0
  ppp authentication chap
  end
  
  The memory leak occurs when a link is flapped up and down.
  Workaround: There is no workaround.
  ```

- **CSCte78406**
On the Cisco ASR 1000 Router console the following error message has been logged on the new standby RP, when PTA sessions are established:

*Feb 2 10:21:36.635: %COMMON_FIB-3-FIBIDBINCONS2: An internal software error occurred. Virtual-Access2.1 linked to wrong idb Virtual-Access2.1

This condition may occur, once PTA sessions are established when performing a RP switchover. After both RPs are synced up with flapped sessions. The error messages are logged on the new standby RP.

Workaround: There is no workaround.

- CSCte78938
  Xconnect configuration is rejected after replacing the MPLS xconnect configuration with manual L2TPv3 configuration on the ASR 1000 Router Series.
  This condition has been seen, when EoMPLS xconnect is configured, while trying to modify the configuration to use L2TPv3 Xconnect on the router.
  Workaround: Do not configure L2TPv3 on an interface which previously was used for EoMPLS.

- CSCte82240
  SBC accepts “.” when key_addr_type is “DIALED_DIGITS”. This condition can occur, when set exact matching means has been set as:
  rpsRtgActionKeyAddrWildcardType to AMB_MW_EXPLICIT_WILDCARD.
  This is possible to have a “.” when rpsRtgActionKeyAddrType is set to AMB_MW_ADDR_TYPE_DIALED_DIGITS. However, it is no longer allowed when rpsRtgActionKeyAddrWildcardType is AMB_MW_EXPLICIT_WCARD (which means SBC should perform an explicit match).
  Workaround: There is no workaround.

- CSCte83888
  When PoD request contains target Acct-Session-Id prepended with NAS-Port-ID it will not be honored.
  This condition has been observed, when PoD prepended is configured with NAS-Port-Id for target sessions.
  Workaround: Is to use only the Session-Id which is located after the, “_” in the Account-Session-ID to specify the session needing disconnect.

- CSCte95396
  A subscriber cannot enable the SSS session due to DPM not finding the binding in the DPM table although the DHCP binding exists as shown by performing the `show ip dhcp server binding` command.
  Debug sss policy event/err would show **SG-DPM: DHCP Binding does not exist query session**.
  This condition is observed when doing the following steps:
  - Subscriber has dhcp binding after initiating `show ip binding` ...
    note: also check the vrf (if any).
  - Subscriber has no entry in the dpm policy.
  - Session trigger needs to be l2-connect dhcp
  Workaround:
- If this is a “slow lease time and relay dhcp case”, make sure subscriber does not send a DHCP packet:
  waiting for the DHCP binding to disappear (i.e., expire), re-enable the user's dhcp forwarding path.
- If this is a “dhcp server” case, clear dhcp binding on the ISG.
- Reload the router

- CSCte97907
  On a Cisco ASR 1000 Router (RP2) may get out of sync with NTP master every 18 minutes for approximately 1 minute. This may offset the NTP Master which will cause an increase up to -1052.1 msec and the sync will get lost.
  This instance has been observed, when NTP is enabled and running apr. 20 minutes.
  Workaround: There is no workaround.

- CSCtf01618
  A Cisco ASR 1000 Series Aggregation Services router may unexpectedly reload due to SegV error.
  The symptom is observed when the router is running Cisco IOS Release 12.2(33)XND1, or later
  XND, or later 12.2(33)XN, and running DMVPN with tunnel protection.
  Workaround: Move to an unaffected release or remove tunnel protection.

- CSCtf04257
  On a Cisco ASR 1000 running IOS XE 12.2(33)XND1 below message may be seen, when trying to configure a EoMPLSoGRE VC:
  %SW_MGR-3-CM_ERROR: Connection Manager Error - provision segment failed
  [SSS:Eth:<number>] - no resources available.
  This condition has been seen on Cisco ASR 1000 Router, running IOS XE 12.2(33)XND1 and under the following conditions:
  - When destination of VC is changed from original to something else and then changed back to original
  - This happens only if we do not exit xconnect submode after the first change and proceed immediately to the second change, then exit via ^Z. The problem does not occur if we exit xconnect submode after the first change.
  Workaround: There is no workaround. If the problem has already occurred, you will need to reload. However, to avoid the problem, exit the config after each change. Do not repeat the same change in the xconenct submode back to back.

- CSCtf05408
  IP address on a loopback interface is lost on the Cisco ASR 1000 Router Series.
  Workaround: Is to reconfigure the loopback interface.

- CSCtf69128
  CRL cache size increases in the multiple of 1024 after each reload
  This condition is observed after configuring the CRL parsed cached size using `crypto ca crl cache size`.
  `show crypto pki crls` will show an incorrect cache size.
  Workaround: There is no workaround.

- CSCtg13269
On peers of Route Reflectors (RR), the received prefixes counter shows an incorrect number when session flaps occur during a network churn.

The symptom is observed with BGP on peers of Route Reflectors (RR's) configured on the ASR 1000 Router.

Workaround: Use the `clear ip bgp *` command.

- **CSCtg35130**

  EIGRP does not come up on a serial interface, on an ASR 1000 Router after reload.

  This behavior is seen, when a serial interface that is part of a VRF after the serial interface is configured with PPP and IP Unnumbered loopback commands, while the interface is part of EIGRP.

  Workaround: The following resolves the issue:

  1) enter `no ip unnumbered loopback` command.
  2) again enter `ip unnumbered loopback` command

- **CSCtg53307**

  The QoS police functionality might fail if user configures both “police” and “priority <kbps>” in the same traffic class.

  This behavior is observed when user configures this unsupported configuration with “police” and “priority <kbps>” in the same traffic class, actually only one police feature is supported per traffic class, and later remove one of the commands, the traffic sent through this class might fail to be policed to the configured rate.

  Workaround: Only enable one police feature in the same traffic class.

- **CSCtg53307**

  The QoS police functionality might fail if user configures both “police” and “priority <kbps>” in the same traffic class. This condition may occur when the user configures this unsupported configuration with “police” and “priority <kbps>” in the same traffic class, actually only one police feature is supported per traffic class, and later remove one of the commands, the traffic sent through this class might fail to be policed to the configured rate.

  Workaround: Is to only, enable one police feature in the same traffic class.

- **CSCth41121**

  An ASR 1000 Router may reload while processing a renegotiation rejection (reINVITE 491) on a call which is being transcoded. This condition occurs when a reINVITE is rejected (a renegotiation failure) on a call which is already established and not using a transcoder. The reINVITE was
attempting to use a transcoder (the new stream needed transcoding). The trigger for this failure is that the renegotiation adds an extra stream to the call (a new m= line in the SDP) and the reINVITE is rejected.

Workaround: There is no workaround.

- CSCth46888
  When the ARP entry is refreshed due to timeout or use of the clear arp command, the router sends ARP request for cached MAC address. However, the request message does not use virtual MAC for Source (Sender) MAC.
  The symptom is observed when the router is VRRP master and VRRP IP is configured the same as the interface IP.
  Workaround: There is no workaround.

- CSCth49844
  Cost extended BGP community is not handled properly on the ASR 1000 Series Router.
  This symptom is observed in the following environment:
  - Paths are received via eBGP.
  - Cost community is set via inbound route-map.
  Workaround: Use bgp bestpath compare-routerid.

- CSCth64122
  When using Lawful Intercept functionality in IOS and you use the cTap2MediationSrcInterface to the set source interface of IAP to MD traffic which is part of a VRF, the VRF’s routing table will not be used, the global routing table will be used instead.
  Workaround: Is to have the source interface of IAP to MD traffic be in the global routing table, not a VRF, or set cTap2MediationSrcInterface to 0 to allow any interface to be used.
  In addition, to fix this behavior: Is to have the source interface updated properly if SNMP input interface object (cTap2MediationSrcInterface) mentioned above is valid. Hence, now the routing will happen using VRF routing table.

- CSCth68125
  SNMP MIBS counter for output/input packets/bytes such as ifOutOctets, ifHCOutOctets, ifHCOutUcastPkts and similar counters will not increment on multiple subinterface. After issuing show vlan counter command this will not allow for the increments to increase on an interface.

  **Note**
  When a large number of subinterfaces are presented under the main interface, the stat update will take a longer time. This may take up to few secs or minutes based on number of subinterface configured with traffic in Cisco IOS XE Release 2.5.0.

  This condition may persist when there are multiple subinterfaces configured and the main interface went into tunnel/L2-transport mode. The above condition has been seen on ASR 1000 Router Series.
  Workaround: There is no workaround for Cisco IOS XE Release 2.5.0.
  For Cisco IOS XE Release 2.6.0 and later releases: Configure hw-module subslot <> ethernet vlan unlimited
  Recovery: Is to perform shut/no shut on the main interface, if this condition still persist then reload the SPA.
Note: The above workaround and recovery mechanism will impact traffic.

- CSCth83143
  IPv6 access list applied to SNMP community string does not work.
  This symptom is observed when an IPv6 ACL is applied to a SNMP Community string.
  Workaround: Is to do the following:
  1. Use SNMP Community string without an ACL.
  2. Use other means to block SNMP access to the device.

- CSCth83442
  When the ASR1002-F Router is functioned as a border router in Performance Routing (PfR) and the
  echo probes are created on the router, the ASR1002-F Router reloads while executing the `show ip sla statistics` or the `show ip sla configuration` commands.
  This condition has been observed when the PfR master controller has learn enabled, there are learn
  lists configured and the policy rule has not applied. The master controller has learned the prefixes
  from the border routers and has instructed the border routers to create the echo probes.
  The border router has learned the prefixes and echo probes are created and sent.
  Workaround: Do not execute the `show ip sla statistics` or `show ip sla configuration` commands.

- CSCth83464
  IPv6 route shows invalid subnet on RADIUS accounting packet.
  This behavior is observed when an IPv6 route statement is entered, the statement that shows up on
  the accounting server is not complete.
  Workaround: There is no workaround.

- CSCti01036
  On the Cisco ASR 1006 a failure may occur during RADIUS Process.
  This behavior is observed after an ASR 1000 Router with RADIUS AAA services is enabled. When
  the RADIUS server sends attributes with no information (empty VSA strings) it produces an
  unexpected reload on ASR 1000 Router.
  Workaround: Is to prevent AAA server from sending empty VSA strings.

- CSCti05663
  A DHCP ACK which is sent out in response to a renew gets dropped at relay.
  The symptom is observed in the case of an numbered relay.
  Workaround: There is no workaround.

- CSCti10518
  Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the rib.
  This condition has been observed when redistribution is occurring into EIGRP and the route
  ownership is changing in the middle of the redistribution process, EIGRP may leak the ndb in
  process.
  Workaround: There is no workaround.

- CSCti30149
  One of the case values in the EIGRP registry is corrupted. This is seen right after bootup.
This symptom is observed when some of the files are compiled with optimization.
Workaround: The corruption is not seen if the files are compiled with optimization disabled.

- **CSCt35960**
  IOS config relating to Persistnet Webui is not picked up during bootup.
  This condition is observed on an ASR 1000 Router with persistent webui config, while rebooting the router.
  Workaround: After boot up, you can render that lost config, and webui does start as usual.

- **CSCt45810**
  A router running Cisco IOS XE Release can experience processor memory leak with AAA enabled as well as SSH. A processes that is showing leaks with in the `show mem` allocating totals include “Dead” and “AAA General DB” processes.
  Another effect of this behavior is that the system failure may occur if an ssh session to the system is attempted while the system is low on memory.
  This condition is observed when SSH and AAA is enabled. Workaround: Change SSH session from password authentication to keyboard interactive authentication.

- **CSCt48014**
  A device reloads after executing the `show monitor event <comp> ... all detail` command (where `<comp>` is an option listed under `show monitor event ?`).
  This symptom is observed if the configurations are done in the order below:
  1. `monitor event-trace <comp> stacktrace <depth>`
  2. `monitor event-trace <comp> size <size value>`
  and any related event gets recorded in between the above two configurations.
  Workaround: To avoid this failure, change the order of the above configurations; that is, configure the “size” command first and then configure the “stacktrace” command.

- **CSCt60740**
  IOS failure may occur after the `disconnect` command is issued.
  This symptoms is observed when the router is accessed through multiple telnet sessions. There may be a chance after issuing `disconnect` command to a telnet session may result in a failure due to the time gap that exists while waiting for the user to hit enter to confirm if telnet session has ended.
  Workaround: Avoid using the `disconnect` command to disconnect a session.
  Alternative: An `exit` command can be used instead.

- **CSCt63499**
  A service policy stays in suspended mode.
  This condition only occurs occasionally after a reload or switchover.
  Workaround: Remove and re-apply the service policy to the interface.

- **CSCt66076**
  A standby HSRP router could be unknown after reloading the ES20 module that is configured for HSRP.
  This symptom is observed under the following conditions:
  - HSRP version 1 is the protocol that must be used.
- Use HSRP with subinterfaces on ES20 module
- Reload the ES20 module

Workaround: Change to HSRPv2, which is not exposed to the issue.

Alternate Workaround: Perform the following steps:

1. Reconfigure HSRP on all subinterfaces.
2. Configure multicast or igmp configuration on the interface where HSRP is configured (like ip pim sparse-mode).

- CSCti74823

Removing an address-family configuration while the prompt is in that address-family sub mode will cause the parser to return to the parent router prompt; however, the parser context values are still set to the address-family context.

This occurs when issuing the command `no address-family vrf “name”` while in `address-family vrf “name”` configuration mode.

Workaround: Exit out of the address-family configuration mode prior to deleting the address-family using the `exit` command and then `no address-family vrf name` command.

- CSCti81291

This is no accounting-start sent by LNS.

This condition is observed when AAA with accounting delayed-start, while LNS is configured for IPv4 *and* IPv6 on the virtual-template Client only negotiates IPv4.

Workaround: There is no workaround. There is an optimal workaround when doing the following:

- Remove ipv6 from vtemplate
- Remove delayed-start
- If the IP address is provided by RADIUS, you can remove the requirement for delayed-start by adding:
  
  > aaa accounting include auth-profile framed-ip-address
  > aaa accounting include auth-profile framed-ipv6-prefix
  > aaa accounting include auth-profile delegated-ipv6-prefix.

- CSCtj00039

Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

Workaround: Clear the route on the PE router using `clear ip route vrf <xxx x.x.x.x>`.  

- CSCtj15805

Keepalive functionality not working. An ICMP echo reply coming back from a client is ignored by ISG.

The symptom is observed when a VRF mapping service is used.

Workaround: There is no workaround.

- CSCtj46144

After issuing the command `show platform` when PEM PRU is displayed on an ASR 1006 Router console: 2RU FM
The symptoms are observed with the following steps:
1. After ASR1006-PWR-DC is removed.
2. Running 12.2(33)XNF2a
Workaround: There is no workaround.

- **CSCtj48387**
  After a few days of operation, an ASR 1000 Router running as an LNS box may not activate with DHCP related errors. The behavior is observed when DHCP has been enabled and while sessions are receiving DHCP information from a RADIUS server.
  Workaround: There is no workaround.

- **CSCtj49133**
  After attaching a policy-map to a subinterface, the policy-map is then renamed and then the subinterface is deleted. The policy-map definition can not be deleted and still shows up in the running configuration.
  The symptoms are observed with the following steps:
  1. Attach a policy to a subinterface.
  2. Rename the policy-map.
  3. Remove the subinterface.
  4. Removing the definition of policy-map will not succeed.
  Workaround: Remove the service policy from subinterface before removing the subinterface.

- **CSCtj56142**
  ISG uses dummy user-name within EAP re-authentication related access-requests as the session identifier. The symptom is observed during EAP re-authentications and likely after CoA-based service activation on an EAP-authenticated session. This happens only when the EAP access-requests carry a dummy user-name and access-accept does not have the correct username.
  Workaround: There is no workaround.

- **CSCtj61252**
  Router failure may occur when bringing up PPP sessions.
  The symptom is observed when adding QoS classes using parametrized QoS attributes where a class name to be added happens to be sub-string of an already existing class.
  Workaround: Do no add or configure class names which are sub-strings of other classes on the router.

- **CSCtj73536**
  Traffic will be stopped to forward to PPP users when PPP users has been terminated on an ASR 1000 Router with L2TP Tunnel configured.
  This behavior happens only when flapping has occurred on a virtual-access interface, several times.
  Workaround: There is no workaround.

## Open Caveats—Cisco IOS XE Release 3.1.1S

This section documents possible unexpected behavior by Cisco IOS XE Release 3.1.1S
- **CSCta31582**
  The `ip flow-export version 9 bgp-nexthop` command by itself has no effect meaning no BGP nexthop information is placed into the Netflow cache or records as a result of the bgp-nexthop token. If instead the commands `ip flow-export version 9 origin-as bgp-nexthop` or `ip flow-export version 9 origin-as bgp-nexthop` are issued, then BGP nexthop information is included in all cases.

  This instance can occur on any ASR 1000 Router platform running the NetFlow feature.

  Workaround: The workaround is covered in the above description. If BGP Nexthop info is desired configure either `origin-as` or `peer-as` in the exporter command and this will cause BGP Nexthop information to appear in the cache and the export records.

- **CSCte98201**
  When `show network-clock` indicates a valid BITS clock state as `valid but not present` on the ASR 1000 Router Series.

  When a valid state BITS clock is removed and re-added in non-revertive mode, then `show network-clock` indicates BITS state as `Valid but not present` even though the Active Source indicates as BITS.

  Workaround: There is no workaround. This seems to be a display issue with the `show network-clock` cli output due to the fact that BITS is indicated as the Active Source.

- **CSCtf01109**
  The NAS-IP-Address value in the `accounting start` changes after an RP SSO. Before the RP SSO, the NAS-IP-Address contains the IP address of the interface connected to the AAA server. After an RP SSO, the new active RP sends out a new accounting start. This time, the NAS-IP-Address contains the loopback 0 IP address. When the session disconnects, the accounting stop record contains the correct IP address.

  The symptom is observed in a redundant RP system with PPP subscribers.

  Workaround: There is no workaround.

- **CSCtf84146**
  An interface may not be cleanly deleted on the ESP board, but is deleted in IOS on the RP. This can be detected via the following command (when run against a subinterface which has previously been deleted via IOS):

  ```
  router-6ru#sh plat hard qfp acti int if-name Tunnel10
  ```

  General interface information
  ```
  Interface Name: Tunnel10
  Interface state: VALID
  Platform interface handle: 30
  QFP interface handle: 25
  Rx uib: 245748
  Tx uib: 245735
  Channel: 0
  ... 
  ```

  On an ASR 1000 Router Series the removal of subinterface with an FNF-NBAR configuration still attached may not cause the subinterface to be removed on the ESP.
Workaround: Remove the FNF-NBAR configuration before deleting the subinterface.

Once in the problem state:
1. config from qfp can be removed like this:
   a. create the interface again,
   b. attach same flow monitor,
   c. remove flow monitor,
   d. remove interface.
2. if the same flow monitor needs to be attached.
   a. create the interface again,
   b. attach same flow monitor,
   c. remove flow monitor,
   d. attach same flow monitor again.
3. Reload the ESP.

- CSCtg47777
  CPU utilization goes high while executing sh command with scaling configuration.
  This condition has been seen when scaling BFD with 128 peers configured on the router.
  Workaround: There is no workaround.

- CSCth42453
  SIP endpoints with shared line appearance fail to receive incoming call properly after an Cisco ASR 1000 Router failover.
  This instance has been observed when SBC CUBE(SP) is running on an ASR 1000 Router. There is no impact to normal SIP endpoint services.
  Workaround: There is no workaround.

- CSCth45402
  When configuring flow exporter VRF destination the port setting is ignored.
  This condition has been observed when a flow exporter has a destination VRF configured but the VRF does not exist.
  Workaround: Do not apply VRF configuration to flow exporter for VRFs that do not exist.

- CSCth47092
  Some classification related show commands could take long time to complete, when the configuration is large. The slowness of the show commands could make the system looks like halt.
  For an example, when executing `show tech` command.
  This condition has been observed when the configuration in device is large.
  Workaround: There is no workaround.

- CSCth50504
  The CUBE(SP) product reloads when configured with a large number of adjacencies, traffic is initiated, and then the entire SBC is deactivated with `no activate`.
  This condition has been observed when scaled configuration is under load.
  Workaround: Remove the traffic from the system before completely deactivating.
Caveats in Cisco IOS XE 3.1S Releases

- CSCth54285
  Remark statement in IPv6 ACL creates a dummy ACE entry in the tcam.
  This instance can occur when presence of remark statement entry is in IPv6 ACL.
  Workaround: There is no affect on functionality.

- CSCth55640
  CE to CE ping failed over when EoMPLS is configured is configured in the native vlan interface
  This conditions has been observe when CE to CE ping failed after EoMPLS is configured in the native vlan interface.
  Workaround: This issue not seen while unlimiting the vlan range by using the CLI `hw-module subslot < > ethernet vlan unlimited`.

- CSCth68986
  Embedded Services Processor (ESP) may be reloaded. This condition may occur when executing a specific configuration sequence by adding and deleting `bandwidth` and `shape` command in the same traffic class, ESP might hit internal error and gets reloaded.
  Workaround: Remove QoS service-policy before modifying policy-map configuration, then reattach the service-policy back to interface.

- CSCth83070
  Invalid error message in the IOS log and there is no impact to the functionality. This condition may happen after enabling APS when running a few switchovers triggered by OIR. In addition after disabling APS and then enable it again may cause the error to occur.
  Workaround: There is no workaround.

- CSCth83442
  When the ASR1002-F Router is functioned as a border router in Performance Routing (PfR) and the echo probes are created on the router, the ASR1002- F Router reloads while executing the `show ip sla statistics` or the `show ip sla configuration` commands.
  This condition has been observed when the PfR master controller has learn enabled, there are learn lists configured and the policy rule has not applied. The master controller has learned the prefixes from the border routers and has instructed the border routers to create the echo probes. The border router has learned the prefixes and echo probes are created and sent.
  Workaround: Do not execute the `show ip sla statistics` or `show ip sla configuration` commands.

- CSCth89976
  Applying monitor with valid exporter and flow record to an interface does not take effect, `show flow exporter template` shows blank output.
  This condition may be seen when configuring FNF monitor on ASR 1000 Router with redundant RPs. The monitor should have a valid exporter and flow record with it. These config actions take place on the active RP. Now do a switch over. Apply monitor to an interface on the newly active RP, after switchover. The monitor may not be correctly applied to the interface.
  Workaround: Delete the flow record and monitor and re-apply.

- CSCth92727
  RTCP traffic in send_only mode is not policed to 5% of tman.
  This condition has been observed when an RTCP pinhole in send_only mode is established, and transmitted traffic has occurred.
Workaround: There is no workaround for this issue. The issue does not impact call rate or quality, but the flow stream will not be policed below the default rate for RTCP traffic.

- CSCth92832
  When a TE tunnel is shut down on a PE router traffic can still flow from the remote PE to the CE behind the shutdown TE tunnel.
  For an example:
  1. The tunnel is shut down on PE1.
  2. Traffic can still flow uni-directionally from CE2 to CE1.
  3. Traffic from CE1 will be dropped on ingress at PE1.
  
  This condition has been observed when EoMPLS is configured with MPLS signaling provided by a MPLS-TE tunnel.
  Workaround: Issue `clear xconnect all` on the remote PE after the TE tunnel is down to cause the remote PE to correctly drop traffic on ingress.

- CSCth96004
  BGP derived Netflow fields (Origin AS, Peer AS, BGP Nexthop) display incorrectly as zero when egress netflow is enabled on an interface in the case where the packets entered on the ASR 1000 Router as MPLS encapsulated packets and are exiting on an ASR 1000 Router as (non-MPLS) IPV4 packets.
  For example:
  Interface configuration for egress netflow can be either
  `ip flow egress`
  or
  `mpls netflow egress`
  To display the records in the Netflow cache the verbose form of the show command is used.
  `show ip cache verbose flow`
  This condition has been observed when the network topology is that for a typical Service Provider application where on an Cisco ASR 1000 Router that is configured as the PE and is sending packets to another router or host which is configured as the CE. The ASR PE-CE interface is configured for IPV4 only and has egress netflow configured on it. Packets entering the ASR 1000 Router must be MPLS encapsulated for this defect to be visible. If the packets entering the ASR 1000 Router are simple IPV4 packets the defect is not seen. Also the defect is not seen for packets taking the reverse path which is to say ingress netflow configured on the PE-CE interface where packets enter the box as IPV4 and leave as MPLS encapsulated packets.
  Workaround: There is no known workaround for Egress Netflow. Some information can be obtained by running ingress Netflow on the PE-CE interface. Also, as noted, if packets entering the box are IPV4 only, egress Netflow functions normally.

- CSCth96398
  Static Global MPLS routes may change labels after SSO causes traffic to drop on the ASR 1000 Router Series.
  This condition may occur when static global mpls routes change labels after SSO causes the traffic to drop on the router.
  Workaround: There is no workaround.

- CSCti09658
Some of the SRTP calls were hung after RTP with SRTP traffic exceeds the max support rate.
This conditions may occur when RTP with SRTP traffic exceeds the max support rate.
Workaround: There is no workaround.

- **CSCt10518**
  Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the rib.
  This condition has been observed when redistribution is occurring into EIGRP and the route ownership is changing in the middle of the redistribution process, EIGRP may leak the ndb in process.
  Workaround: There is no workaround.

- **CSCt27989**
  An ASR 1000 Router may show incorrect stats for exporter clients.
  This will happen when an exporter has multiple clients, for example an exporter being used by two flow monitors at the same time.
  Workaround: Use only one client per exporter.

- **CSCti45918**
  Show ip mroute vrf abc x.x.x.x count displays zero packets for an active m-cast stream.
  This condition has been observed when then DMVPN spoke tunnels are in a vrf instance and the tunnel source interface is in global table.
  Workaround: Enable `ip pim sparse-mode` on tunnel-source interface in global table.

- **CSCti48585**
  Loss of connectivity on a SPA-4XCT3/DS0 when performing a manual ISSU subpackage upgrade on ESP's in an Cisco ASR 1000 Router. This condition has been observed upon performing a manual ISSU subpackage upgrade from version IOS XE 2.4.4 on the ESP's with SPA-4XCT3/DS0 configured this may cause the traffic to stop passing.
  Workaround: Perform the upgrade using a consolidated package method or by loading packages from packages.conf and reload.

- **CSCti57128**
  When CUBE(SP) is configured on the Cisco ASR 1000 Router, during an upgrade the configuration using header-profiles which reference privacy headers or privacy parameters fail to migrate correctly.
  An error is generated stating that cac-policy should be used to modify privacy settings. However no `cac-policy` commands exist to allow the re-configuration.
  For example:
  
  ```
  sbc <name> 
  sbe 
  sip header-profile <name> 
  header Privacy 
  header-Remote-Party-ID
  ```
  Workaround: The solution allows seamless upgrade of these commands.

- **CSCti59562**
  DHCP accounting stop does not clear IP initiated session and radius-proxy sessions after CoA account logon / logoff / logon sequence. This condition has been observed when VRF mapping is being used on an Cisco ASR 1000 Router.
Workaround: There is no workaround.

- **CSCti62355**
  An unexpected reload may be seen on an ASR 1000 Series with Flexible Netflow configurations containing multiple flow monitors with exporters.
  This condition may occur on a router that has IP unicast and multicast configured, when multiple monitors are configured for flow monitoring by attaching them to one or more interfaces, issuing a `show ip cache flow` can result in an ESP reload.
  Workaround: There is no workaround.

- **CSCti70690**
  SBC causes ASR 1000 to reload, hitting CHECK failure (dumping diagnostics) and then an unhandled exception.
  The condition has been seen if CHECK and reload (exception) occurs when the following call flow takes place:
  - A call is made and successfully answered.
  - The callee chases the 200 INVITE response immediately with a BYE request. (These messages are so close together that they are processed by SBC in the same N-BASE schedule.)
  - SBC hits a CHECK failure while processing the BYE request, and passes on the 200 INVITE response.
  - The caller receives the 200 INVITE and sends an ACK.
  - SBC hits an unhandled exception while processing the ACK from the caller.
  This also requires that there is a subscriber registered through an ASR 1000 Router; or that a switchover has been performed, otherwise the failure is not seen when this flow occurs.
  Workaround: Do not use core with access type adjacencies.

- **CSCti76872**
  Interface names are truncated in the Flexible Netflow feature CLI output, such as in the following example:
  ```
  Auto-MCP2#sh run int gigabitEthernet 0/2/6.6666666
  Building configuration...
  Current configuration : 129 bytes
  
  interface GigabitEthernet0/2/6.6666666
  encapsulation dot1Q 6
  ip vrf forwarding vpn6
  ip address 115.0.6.1 255.255.255.255.0
  end
  ```
  ```
  Auto-MCP2#sh ip cache flow
  SrcIf | SrcIPaddress | DstIf | DstIPaddress | Pr SrcP DstP Pkts
  Local | 15.1.1.4 | Tunnel4* | 224.0.0.10 | 58 0000 0000 71
  Tunnel3 | 113.0.3.2 | gi0/2/6.3 | 115.0.3.2 | ff 0000 0000 548 K
  ```
  This condition may be seen when Flexible Netflow on the ASR 1000 Router Series on “long” interface names.
  Workaround: There is no workaround.

**Resolved Caveats—Cisco IOS XE Release 3.1.1S**

All the caveats listed in this section are resolved in Cisco IOS XE Release 3.1.1S
• CSCtb58282
  Device running IOS may reload when show tcp brief is issued.
  This condition as observed when the following has occurred:
  1. The “ip domain lookup” command needs to be configured. It is on by default.
  2. The ip address of the foreign host in the tcp session needs to have a very long domain name
     associated with it, on the order of 70 characters.
  3. The port number of the foreign host needs to be 5 digits long.
  If ip domain lookup is disabled, the problem could still happen if the host has a static entry
   configured with the ip host command.
  Workaround: Configure no ip domain lookup or avoid using show tcp brief on the device.

• CSCtf05408
  IP address on a loopback interface is lost.
  Workaround: Reconfigure the loopback interface.

• CSCtg11491
  System may encounter CPUHOG and an error message with the following traceback:
  %SYS-3-CPUHOG: Task is running for (2302)msecs, more than (2000)msecs (1/1), process = Exec
  After clearing 4k+ ISG RADIUS Proxy sessions through the CLI: clear radius-proxy client <ip address>.
  This symptom is observed on a Cisco ASR 1000 Router Series when functioning as an Intelligent
  Service Gateway (ISG) RADIUS Proxy after thousands of sessions are established.
  Workaround: There is no known workaround.

• CSCtg30995
  Delay of RP switchover associated with NV_BLOCK_INITFAIL message is appearing on standby
  turned-active RP console.
  This problem may occur when the manual switchover command, redundancy force-switchover and
  a filesystem command like copy running-config startup-config is issued from different Active RP
  consoles almost at the same time.
  Workaround: Avoid issuing any filesystem access command simultaneously with the manual RP
  switchover command. Should the above problem occurs, execute the same filesystem command, by
  issuing copy running-config startup-config from the standby-turned-active console.

• CSCtg52483
  SPA-1XCHOC12/DS0 reloads while BERT is running on the same results into malfunctioning of
  the router.
  This condition has been observed while BERT test is running, the SPA OIR resulted in BERT test
  hanging situation and afterwards the router does not allow for the BERT test to start anew. In
  addition, the previous BERT run is shown in running state even when no bert command is issued to
  stop the sequence.
  Workaround: There is no workaround.

• CSCth25661
  Plim qos scheduling commands disappear from running config on the standby RP if the SPAs
  stopped while the standby is down.
The following are the steps which may likely cause this problem:

1. Bring the standby RP down.
2. Configure an interface on the active RP.
3. Stop the SPA.
4. Bring the standby up.
5. Switchover to the standby RP and start the SPA.

Workaround: Stop the SPA when the standby is up and perform a switchover.

- **CSCth50961**
  POS configuration is not supported on the SPA-1XCHSTM1 SPA. However if you have the unsupported configuration on this SPA the router may fail repeatedly when booting the router.
  Workaround: Is to remove the unsupported POS configuration.

- **CSCth59072**
  After reloading ASR 1000 Router the backup interface is stuck to up instead of standby sometimes.
  This happens when using IOS XE 2.4.2 Release, or possibly later IOS XE releases.
  Workaround: Is to flap the affected interface.

- **CSCth62425**
  When trying to add a static and extendable NAT rule for port 80 or 443 (PAT), the operation fails with this error message:
  
  %Port 80 is being used by system min80
  or
  %Port 443 is being used by system min443

  This condition has been observed when upgrading from IOS Release 12.2(33)XND to 12.2(33)XNF and the following has occurred:
  - Add NAT rule for either port 80 or 443.
  - Delete NAT rule.
  - Add the same nat rule with a different Inside Local address.
  - Delete NAT rule.
  - Try to add the original NAT rule.
  - At this point, no other static nat rule can be added with the same Inside Global and port 80/443

  Workaround: Perform the following steps:

  1. Make sure that the HTTP port and secure-port are assigned to other than 80 and 443, respectively, and enable them.

     For example:
     
     ip http port 10500
     ip http secure-port 11000
     ip http server
     ip http secure-server

  2. Configure the port static mappings for the above ports for 80 and 443.

     For example:
3. Change these HTTP ports back to 80 and 443.
For example:

```
ip http port 80
ip http secure-port 443
```
4. Afterwards, the above port static mappings can be deleted and then added again, normally.

- **CSCth64507**
  Bulk Sync failure is seen on redundancy force-switcover command when eem policy is configured and policy file is present in only the Active RP.
  The failure is seen only when the policy file is present in a Active RP and not in a Standby RP.
  Workaround: Is to have the policy file present in both the Active RP and Standby RP.

- **CSCth70149**
  Wr mem fails after entering the command `verify nvram:startup-config` on a Cisco ASR 1000 Router.
  The following example identifies a Cisco ASR 1000 Router that is running Cisco IOS Software Release 12.2(33)XNE2:
  ```
  router#verify nvram:startup-config
  Verifying file integrity of nvram:startup-config...
  Embedded Hash   SHA1 : 0A210A21204C61737420636F6E66696775726174
  Computed Hash   SHA1 : 523416EF6B0CE417B3E12FFBA3491131B8821234
  Embedded hash verification failed for file nvram:startup-config.
  router#
  MEST: %SIGNATURE-3-NOT_VALID: %ERROR: Signature not valid for file nvram:startup-config.
  Router#wr
  startup-config file open failed (Device or resource busy)
  This condition has been seen when the ASR 1000 is running 12.2(33)XNE2.
  Workaround: Is to reload the router.

- **CSCth70566**
  %ASR1000_RP_SPA-3-VC_FLOWID_ALLOC_FAIL messages are shown on the console after RP switchover.
  The issue may happen if additional ATM PVCs are configured and an RP switchover has happened.
  Workaround: There is no workaround.

- **CSCth72829**
  When trying to enable Virtual Fragmentation Reassembly feature the same in the interface level configuration is unable to be seen.
  As shown in the following configuration example:
  ```
  ASR(config)#int gig 2/0/0
  ```
ASR(config-if)#ip v?
verify vrf
This condition may occur when the ASR 1000 is running IOS XE using IPBASE feature sets.
Workaround: None

- CSCth96093
When the Cisco ASR 1000 platform is configured with Fast Re-Route for Traffic Engineering purposes the router will lose their backup tunnel after performing ISSU procedure. The primary tunnel will continue to function and there is no permanent traffic loss. However, if the primary tunnel fails for any reason, there will be no backup tunnel to fall back on.

The problem may happen when ISSU downgrade from an IOS XE version 3.1.1S or higher to version 3.1.0 is done, after a redundancy forced switchover in the ISSU procedure.

Workaround: The problem can be addressed by re-applying the traffic engineering backup-path command on the interface after the ISSU downgrade and after the box has been forced onto the newly downgraded route processor.

For example:
MCP-6RU-2(config-if) # mpls traffic-eng backup-path <Tunnel #>

- CSCti01831
Standby ESP may get stuck in init state.
This condition has been observed after performing an ISSU downgrade to a IOS XE 3.1S image.
Workaround: There is no workaround.

- CSCti05253
When POS interface has been created using SPA-1XCHOC12/DS0 the SPA is no longer accessible, after performing an OIR for the slot in which the SPA is present.

This instance may always occur whenever an OIR has performed in the slot in which the SPA-1XCHOC12/DS0 is present.

Workaround: There is no known workaround.

- CSCti05925
The DTMF interworking function of IPIP gateway is not working, properly. The DTMF relay of one format converts to another DTMF relay format by IPIP gateway

The problem may exist on the ASR 1000 platform or other platforms when running BINOS.

Workaround: There is no workaround.

- CSCti06235
Firewall cannot send out HSL packets on ESP40. The destination IP is reversed in the datapath.

This condition may occur after configuring Firewall HSL on ESP40.

Workaround: Configure a reversed destination IP.

- CSCti10146
On injecting LAIS into POS interface, PRDI is seen together with LAIS.

This issue has been seen on an Cisco ASR 1000 Router running IOS XE Release versions, staring from 2.5.0 and onwards.

Workaround: There is no workaround.
CSCti41837
Clear Channel POS interface configured on Channelized OC12 card might stay up/down in case of Path alarms.
This condition has been observed when the following steps have been executed:
1. Insert Path alarm such as PAIS with path delay triggers enabled
2. Insert Line alarm such as SLOS
3. Remove Line alarm
The above steps would result in POS interface being stay up/down in case Path alarm PAIS present.
Workaround: Controller `sh/no sh` would bring POS interface back to down/down state.

CSCti58920
The following error message is observed when SPA-4XT-SERIAL is housed in ASR1000-SIP40:
`%SPA_OIR-3-UNSUPPORTED: The SPA-4XT-SERIAL (0x55A) in subslot 0/0 is not supported by the ASR1000-SIP40 module`
The symptom is observed when SPA-4xT-Serial SPA is configured on the ASR1000-SIP40 running Cisco IOS XE 3.1.0S Release.
Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.1.0S

This section documents possible unexpected behavior by Cisco IOS XE Release 3.1.0S

CSCsz79432
While sending traffic from the RTR1 to RTR2 outgoing interface network, RTR2 is not forwarding directed broadcast when enabling ip directed-broadcast on an ASR 1000 Router.
This condition has been observed when enabling ip directed-broadcast on the router, while sending traffic from the RTR1 to RTR2 outgoing interface network, RTR2 is not forwarding directed broadcast.
Workaround: There is no workaround.

CSCsz82080
Under a scaled configuration (e.g. 1500 DVTI remote access sessions), when bringing up all the 1500 sessions at the same time in the DVTI server, the ESP may also reload.
This condition has been observed when bringing up 1500 DTVI sessions simultaneously.
Workaround: Is to bring up 100 Virtual Access interfaces at one time.

CSCtg18977
RP reloads when it detects that the control plane has locked up.
This condition occurs with a high amount of punted traffic specifically when the system is running with LARGE amount of BGP sessions.
Workaround: There is no workaround.

CSCtg60941
When attempting to establish a BGP adjacency from an interface in an IPv4 VRF address family to a peer accessible through the global routing table fails.
This is occurs when one neighbor IP address is in a VRF address family and the other neighbor address is accessible via the global routing table using static routes to leak the routes between the two routing tables.

Workaround: There is no workaround.

- **CSCtg78972**
  Memory Leak in FMAN-ESP ACL.
  The memory allocated by “acl” module in FMAN-ESP keeps growing by ~128 bytes for each ~28K PPPoEoA flapping.
  This condition may occur when there are flapping PPPoEoA sessions.
  Workaround: There is no workaround.

- **CSCtg88383**
  ESP40 occasionally gets stuck in “init, active” state during reboot.
  This problem is seen during ESP reboot.
  Workaround: No workaround is required. After about 300 seconds, RP reboots ESP40 and ESP40 comes up fine next time.

- **CSCtg90378**
  An Cisco ASR 1000 Router may take ~18 - 20+ minutes to boot completely and during the course the IOS CUP remains high at 99.9%.
  This condition may be seen with high FW and NAT scaled configurations.
  Workaround: There is no workaround.

- **CSCtg95994**
  MLP bundle interface fails to come up properly with the following error message:
  QFP:00 Thread:126 TS:00000002037602773659 %QFP_MLP-3-PROXY_DUP_LINK_ID:
  QFP MLP Proxy (Rx LINK-ADD) duplicate Link ID ...
  and will not forward traffic.
  This can occur if a MLP bundle with multiple member links is torn down and recreated several times.
  Workaround: There is no workaround.

- **CSCth08631**
  When the outbound traffic is fragmented packets, the second and on-going fragments do not contain any L4 information about the ASR 1000 Router. However, there maybe some false positive matches on an output ACL.
  This condition are observed when outbound traffic is fragmented packets and some false positive matches on an output ACL has occurred.
  Workaround: Create very specific ACLs using specific IPs for all entries that are not scalable.

- **CSCth11310**
  IP-subscriber sessions stop forwarding traffic after RADIUS proxy resets them. The session does not appear to get any traffic, and drops may be observed when the following command is used:
  show platform hardware qfp active statistics drop
  This behavior may occur on ASR 1000 Router Series, with routed IP-subscriber sessions that are reset and converted to RADIUS proxy sessions.
Caveats in Cisco IOS XE 3.1S Releases

Workaround: There is no workaround.

- CSCth24984
  High CPU usage on when RP1 is configured as the DMVPN hub. This condition may occur when having 1000 Static BGP neighbors (spokes) over the DMVPN hub.

  Workaround: There is no workaround.

- CSCth27728
  After SBC has been configured on an ASR 1000 Router, and a SIP call is made. The router reloads. This condition has been seen when the del-prefix 0 instructs SBC to remove the first zero digits from a dialed number, which means not doing anything. SBC does not handle being instructed to remove zero digits from the number and this is may cause a failure. Removing this from the config should result in the same behavior and may avoid the router to fail.

  Workaround: By removing edit del-prefix 0 add-prefix 64 from the config and replacing it with edit del-prefix 1 add-prefix 64 this should prevent the router from failing.

- CSCth36539
  IPv6 Video on demand traffic is not forwarded by ESP 40.

  This condition can occur when the number of VoDv6 are scaled (> 300 sbc pinholes), traffic for IPv6 VoD destinations will not be forwarded by ESP 40.

  Workaround: Is to reduce the number of VoDv6 pinholes to 1.

- CSCth37116
  IP Accounting feature is not supported on the Cisco ASR 1000 Router Series. This only applies to the Cisco ASR 1000 Router Series.

  Workaround: Do not configure IP Accounting on Cisco ASR 1000 Router Series.

- CSCth41121
  An ASR 1000 Router may reload while processing a renegotiation rejection (reINVITE 491) on a call which is being transcoded. This condition occurs when a reINVITE is rejected (a renegotiation failure) on a call which is already established and not using a transcoder. The reINVITE was attempting to use a transcoder (the new stream needed transcoding). The trigger for this failure is that the renegotiation adds an extra stream to the call (a new m= line in the SDP) and the reINVITE is rejected.

  Workaround: There is no workaround.

- CSCth41321
  Standby ESP reloads after repeated RP switchovers. This conditions has been seen when PPPoX sessions with ISG features in a dual RP with dual ESP configuration. After many repeated switchovers have occurred while sessions continue to be setup, the standby ESP may fail.

  Workaround: No known workaround.

- CSCth43945
  QFP might reload when scaled configuration of GRE with QoS is loaded, and the physical interface state is up/down quickly.

  This condition has been observed when the ASR 1000 is configured with a large number of GRE tunnels with QoS service-policy, and the physical port used by the GRE tunnels have experienced the link state up/down within a short interval, the QFP might be reloaded due to one critical process getting reset.

  Workaround: There is no workaround.
• CSCth45487
On a Cisco ASR 1000 Router a cpp_cp_srvr reload has been observed while booting up with NAT configurations.
This problem may occur on the router when there are high amounts of traffic sent, and low memory condition occurs.
Workaround: There is no workaround.

• CSCth48147
SBC hits a CHECK failure (and dumps diagnostics files) when processing a BYE rejection response.
This CHECK failure occurs (on SBC version 2500_065) when the following call scenario takes place:
  − A call is set up between caller and callee. SIP to SIP call. Delta renegotiation is configured (the default behavior).
  − A reINVITE, which changes the media (for example, a codec change) is sent from the caller and received at the callee. No response is yet sent.
  − A BYE is sent from the caller to the callee. No response is yet sent.
  − The callee then responds to the reINVITE with a 481 error code. This causes SBC to start to tear down the call.
  − Immediately after sending the 481 reINVITE response, the callee sends a 491 BYE response (the same reload occurs if this is some other error codes, but it must not be 481 or 200). When SBC processes the 481 reINVITE response and 491 BYE response in quick succession, the Check failure occurs.
Workaround: None

• CSCth48281
SBC reloads when processing a 302 INVITE response. This is due to a problem on a forked call previously.
Reload occurs after a forked call in which SBC processes two incoming calls with the same Call-ID and From tag. One of these calls is answered and before either an answer on the other call or an ACK on the first call, the callee sends a BYE to SBC. SBC fails due to being unable to correctly correlate the BYE with the right call.
Workaround: There is no workaround.

• CSCth48869
Console Freeze (Lock) and iosd CPU remains at 99.9% for more than 45 minutes. This happens when unconfiguring and reconfiguring QoS on the interfaces which are configured for NAT / FW redundancy. This happens when 75 - 200 interfaces are unconfigured and configured for QoS.
Workaround: There is no workaround.

• CSCth50961
POS configuration is not supported on the SPA-1XCHSTM1 SPA. However if you have the unsupported configuration on this SPA, the router reloads repeatedly when the router is booted.
Workaround: Remove the unsupported POS configuration.

• CSCth53652
SBC reloads while processing a BYE response from an endpoint before a call has been connected when the caller has sent a BYE followed by a CANCEL.
This occurs when the following call flow is seen:

1. INVITE from caller to callee.
2. Callee sends provisional response back (for example, 180).
3. Caller sends BYE to callee.
4. Caller then sends CANCEL to callee.

   This will cause SBC to return 487 INVITE response (and 200 CANCEL) and start call teardown. SBC will also respond 481 to the BYE from the caller, and forward the CANCEL to the callee.
5. Callee then sends 200 BYE response, which causes the problem.

Workaround: There is no workaround.

- CSCth59072

   After reloading ASR 1000 Router the backup interface is stuck to up instead of standby sometimes. This happens when using IOS XE 2.4.2 Release, or possibly later IOS XE releases.

   Workaround: Is to flap the affected interface.

- CSCth60620

   XE31 Kernel core needs to be processed off-router due to utility changes. If a Cisco ASR 1000 Series Router experiences a kernel core, it will require off-loading for processing. Kernel cores are large when compressed (at about 2GB or more) and will expand to 8GB to up to 16GB depending on the RP memory capacity. The utility, crash, used to examine these cores dynamically links to other libraries, so it cannot be run on an ASR 1000 with the same image. There are concerns about storage on the router being sufficient if one could be decoded on an ASR 1000 (easily worked around). Having the correct vmlinux and map file is required.

   Workaround: Use the recommended procedure. Make sure that the target file system supports files of up to 16GB and is running the proper version of Linux.

- CSCth62425

   When trying to add a static and extendable NAT rule for port 80 or 443 (PAT), the operation fails with this error message:

   `%Port 80 is being used by system min80`
   or
   `%Port 443 is being used by system min443`

   Workaround: There is no workaround.

- CSCth66196

   Static NAT with “no-payload” option breaks if zone-based firewall is enabled on the ASR 1000 Router Series.

   Without Zone-based Firewall configured on the router, NAT works.

   Workaround: There is no workaround.

- CSCth67494

   Some packets from captive portal to client are not hitting the redirect translations.

   The precise conditions are not known but this seems to be related to activating/deactivating new services on subscriber session.

   Workaround: There is no workaround.

- CSCth68125
SNMP MIBS counter for output/input packets/bytes such as ifOutOctets, ifHCOutOctets, ifHCOutUcastPkts and similar counters will not increment on multiple subinterface. After issuing `show vlan` counter command this will not allow for the increments to increase on an interface.

**Note**  When a large number of subinterfaces are presented under the main interface, the stat update will take a longer time. This may take up to few secs or minutes based on number of subinterface configured with traffic in Release 2.5.0.

This condition may persist when there are multiple subinterfaces configured and the main interface went into tunnel/L2-transport mode. The above condition has been seen on ASR 1000 Router Series.

Workaround: There is no workaround for Release 2.5.0.

For Release 2.6.0 and later releases: Configure `hw-module subslot <> ethernet vlan unlimited`

Recovery: Is to perform `shut/no shut` on the main interface, if this condition still persist then reload the SPA.

**Note** The above workaround and recovery mechanism will impact traffic.

- **CSCth70149**
  Wr mem fails after entering the command `verify nvram:startup-config` on a Cisco ASR 1000 Router.
  
The following example identifies a Cisco ASR 1000 Router that is running Cisco IOS Software Release 12.2(33)XNE2:
  
  ```
  router#verify nvram:startup-config
  Verifying file integrity of nvram:startup-config...
  Embedded Hash   SHA1 : 0A210A21204C617374206366696775726574
  Computed Hash   SHA1 : 523416EF6B0CE417B3E12FFBA349131B8821234
  Embedded hash verification failed for file nvram:startup-config.
  router#
  MEST: %SIGNATURE-3-NOT_VALID: %ERROR: Signature not valid for file nvram:startup-config.
  Router#wr
  startup-config file open failed (Device or resource busy)
  ```

  This condition has been seen when the ASR 1000 is running 12.2(33)XNE2.

  Workaround: Is to reload the router.

- **CSCth71105**
  ESP20 core after "no SBC" under high rate traffic (CPS=58/HT=180) for RTP with SRTP traffic for an hour.

  This condition has been observed when RTP with SRTP traffic ESP20 after "no SBC" under high rate traffic has occurred.

  Workaround: There is no workaround.

- **CSCth72507**
  When an ASR 1000 Router has attached running config the active secondary keeps reloading.
Workaround: There is no workaround.

- **CSCth72829**
  When trying to enable Virtual Fragmentation Reassembly feature the same in the interface level configuration is unable to be seen.
  As shown in the following configuration example:
  ASR(config)#int gig 2/0/0
  ASR(config-if)#ip v?
  verify vrf
  This condition may occur when the ASR 1000 is running IOS XE using IPBASE feature sets.
  Workaround: None

- **CSCth72869**
  Changes in adjacencies during RP switchover while running WCCP may trigger IOS reload with the following message:
  ASR1000-EXT-SIGNAL: U_SIGABRT(6), Process = Net Background
  The following error may be seen shortly before the reload:
  %FMANRP_OBJID-5-DUPCREATE: Duplicate forwarding object creation obj_handle <hex value>, type <number>, existing obj_id <hex value>, type <number>
  Workaround: Disable WCCP.

- **CSCth72971**
  Unexpected ESP reload may occur, accompanied by the following error message:
  %OOM-3-NO_MEMORY_AVAIL: F1: oom.sh: The system is very low on available memory. Operations will begin to fail.
  The router's configuration includes multiple deny statements.
  Workaround: Remove the deny statements from the config.

- **CSCth73260**
  QFP reload may occur or output indicates 0 translation when there are translations. In addition, a traceback may also occur.
  This occurs upon entering `sh ip nat trans` with more then 250 static networks or upon entering `sh ip nat trans verb` with more then 50 static networks.
  Workaround: Reduce the number of static networks or avoid these commands. This problem is expected to be correct in IOS XE 3.1.1S Rebuild.

- **CSCth75324**
  Throughput degradation is about 8% compared to Release 2.6.0 when MPLS SETVRF feature is configured on the ASR 1000 Router Series.
  In Release 2.6.0, throughput was 12.31 Mpps with RP1/ESP10. However, in Release 3.1.0S, throughput is 11.29 Mpps with RP1/ESP10.
  This condition has been observed when an ASR 1000 is configured with PBR set VRF+L3VPN with 500 VRFs this will cause the throughput performance degradation.
  Workaround: There is no workaround to increase the performance.
The following command: `sh platform hardware slot <slot-num> plim qos input bandwidth` command doesn't display the configured values for policer and weight configuration on CC40.

The problem is seen on CC40 only when it has an ATM SPA. The configured values are not displayed for the other SPAs sitting next to ATM SPA in the same bay but doesn't have any functionality impact.

Workaround: Perform `hw-module subslot <slot/subslot> shut` on the ATM SPA and the configured values can be seen in the `show` command output.

- CSCto03123
  
  Symptoms:
  
  1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
  
  2. Additional memory leak can occur when frequent sensor value changes take place.

  Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:
  
MIBs Used in Cisco IOS XE 3S Releases

To locate and download MIBs for selected platforms, Cisco IOS and Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following location:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:


To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at the following location:


MIBs for the Cisco ASR 903 Series Aggregation Series Router and the Cisco ASR 1000 Series Aggregation Services Routers

- Cisco ASR 903 Series Aggregation Services Router, page 469
- Cisco ASR 1000 Series Aggregation Services Routers, page 473

Cisco ASR 903 Series Aggregation Services Router

The Cisco ASR 903 Series Router supports the following MIBs:

- BGP4-MIB (RFC 1657)
- CISCO-BGP-POLICY-ACCOUNTING-MIB
- CISCO-BGP4-MIB
- CISCO-BULK-FILE-MIB
- CISCO-CBP-TARGET-MIB
- CISCO-CDP-MIB
- CISCO-CEF-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-DATA-COLLECTION-MIB
- CISCO-EMBEDDED-EVENT-MGR-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-EXT-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-SENSOR-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-FLASH-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-IETF-ISIS-MIB
- CISCO-IETF-PW-ATM-MIB
- CISCO-IETF-PW-ENET-MIB
- CISCO-IETF-PW-MIB
- CISCO-IETF-PW-MPLS-MIB
- CISCO-IETF-PW-TDM-MIB
- CISCO-IF-EXTENSION-MIB
- CISCO-IGMP-FILTER-MIB
- CISCO-IMAGE-LICENSE-MGMT-MIB
- CISCO-IMAGE-MIB
- CISCO-IPMROUTE-MIB
- CISCO-LICENSE-MGMT-MIB
- CISCO-MVPN-MIB
- CISCO-NETSYN-C-MIB
- CISCO-OSPF-MIB (draft-ietf-ospf-mib-update-05)
- CISCO-OSPF-TRAP-MIB (draft-ietf-ospf-mib-update-05)
- CISCO-PIM-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-PTP-MIB
- CISCO-RF-MIB
- CISCO-RTTMON-MIB
- CISCO-SYSLOG-MIB
- DS1-MIB (RFC 2495)
The Cisco ASR 903 Series Router supports the following unverified and supported MIBs:

- ATM-MIB
- CISCO-ATM-EXT-MIB

The Cisco ASR 903 Series Router supports the following unverified and supported MIBs:

- ENTITY-MIB (RFC 4133)
- ENTITY-SENSOR-MIB (RFC 3433)
- ENTITY-STATE-MIB
- EVENT-MIB (RFC 2981)
- ETHERLIKE-MIB (RFC 3635)
- IF-MIB (RFC 2863)
- IGMP-STD-MIB (RFC 2933)
- IP-FORWARD-MIB
- IP-MIB (RFC 4293)
- IPMROUTE-STD-MIB (RFC 2932)
- MPLS-LDP-GENERIC-STD-MIB (RFC 3815)
- MPLS-LDP-STD-MIB (RFC 3815)
- MPLS-LSR-STD-MIB (RFC 3813)
- MSDP-MIB
- NOTIFICATION-LOG-MIB (RFC 3014)
- OSPF-MIB (RFC 1850)
- OSPF-TRAP-MIB (RFC 1850)
- PIM-MIB (RFC 2934)
- RFC1213-MIB
- RFC2982-MIB
- RMON-MIB (RFC 1757)
- RSVP-MIB
- SNMP-COMMUNITY-MIB (RFC 2576)
- SNMP-FRAMEWORK-MIB (RFC 2571)
- SNMP-MPD-MIB (RFC 2572)
- SNMP-NOTIFICATION-MIB (RFC 2573)
- SNMP-PROXY-MIB (RFC 2573)
- SNMP-TARGET-MIB (RFC 2573)
- SNMP-USM-MIB (RFC 2574)
- SNMPv2-MIB (RFC 1907)
- SNMPv2-SMI
- SNMP-VIEW-BASED-ACM-MIB (RFC 2575)
- TCP-MIB (RFC 4022)
- TUNNEL-MIB (RFC 4087)
- UDP-MIB (RFC 4113)
- CISCO-ATM-IF-MIB
- CISCO-ATM-PVC-MIB
- CISCO-ATM-PVCTRAP-EXTN-MIB
- CISCO-BCP-MIB
- CISCO-CALLHOME-MIB
- CISCO-CIRCUIT-INTERFACE-MIB
- CISCO-CONTEXT-MAPPING-MIB
- CISCO-EIGRP-MIB
- CISCO-ERM-MIB
- CISCO-ETHER-CFM-MIB
- CISCO-ETHERLIKE-EXT-MIB
- CISCO-EVC-MIB
- CISCO-HSRP-EXT-MIB
- CISCO-HSRP-MIB
- CISCO-IETF-ATM2-PVCTRAP-MIB
- CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN
- CISCO-IETF-BFD-MIB
- CISCO-IETF-DHCP-SERVER-MIB
- CISCO-IETF-DHCP-SERVER-EXT-MIB
- CISCO-IETF-MPLS-TE-P2MP-STD-MIB
- CISCO-IETF-PPVPN-MPLS-VPN-MIB
- CISCO-IP-STAT-MIB
- CISCO-IPSLA-ETHERNET-MIB
- CISCO-L2-CONTROL-MIB
- CISCO-LAG-MIB
- CISCO-MAC-NOTIFICATION-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NHRP-EXT-MIB
- CISCO-NTP-MIB
- CISCO-PING-MIB
- CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB
- CISCO-RTTMON-ICMP-MIB
- CISCO-RTTMON-IP-EXT-MIB
- CISCO-RTTMON-RTP-MIB
- CISCO-SNMP-TARGET-EXT-MIB
- CISCO-TCP-MIB
- CISCO-VRF-MIB
- ETHER-WIS (RFC 3637)
MIBs Used in Cisco IOS XE 3S Releases

- EXPRESSION-MIB
- HC-ALARM-MIB
- HC-RMON-MIB
- IEEE8021-CFM-MIB
- IEEE8021-CFM-V2-MIB
- IEEE8023-LAG-MIB
- INT-SERV-GUARANTEED-MIB
- INTEGRATED-SERVICES-MIB
- MPLS-L3VPN-STD-MIB (RFC 4382)
- MPLS-LDP-ATM-STD-MIB (RFC 3815)
- MPLS-LDP-MIB
- MPLS-TE-STD-MIB
- MPLS-VPN-MIB
- NHRP-MIB
- RFC2006-MIB (MIP)
- RMON2-MIB (RFC 2021)
- SMON-MIB
- VRRP-MIB

For information about the Cisco ASR 903 Series Router product implementation of the MIB protocol, see Cisco ASR 903 Series Aggregation Services Router MIB Specifications Guide at the following location:


Cisco ASR 1000 Series Aggregation Services Routers

The Cisco ASR 1000 Series Routers support the following MIBs:

- ATM-MIB
- BGP4-MIB (RFC 1657)
- CISCO-AAA-SERVER-MIB
- CISCO-AAA-SESSION-MIB
- CISCO-AAL5-MIB
- CISCO-ATM-EXT-MIB
- CISCO-ATM-PVCTRAP-EXTN-MIB
- CISCO-ATM-QOS-MIB
- CISCO-BGP4-MIB (updated to support IPv6 addresses)
- CISCO-BULK-FILE-MIB
- CISCO-CBP-TARGET-MIB
- CISCO-CDP-MIB
- CISCO-CEF-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-CONTEXT-MAPPING-MIB
- CISCO-DATA-COLLECTION-MIB
- CISCO-EMBEDDED-EVENT-MGR-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-EXT-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-PERFORMANCE-MIB
- CISCO-ENTITY-QFP-MIB
- CISCO-ENTITY-SENSOR-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-FLASH-MIB
- CISCO-FRAME-RELAY-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-HSRP-EXT-MIB
- CISCO-HSRP-MIB
- CISCO-IETF-ATM2-PVCTRAP-MIB
- CISCO-IETF-FRR-MIB
- CISCO-IETF-ISIS-MIB
- CISCO-IETF-NAT-MIB
- CISCO-IETF-PPVPN-MPLS-VPN-MIB
- CISCO-IETF-PW-ATM-MIB
- CISCO-IETF-PW-ENET-MIB
- CISCO-IETF-PW-MIB
- CISCO-IETF-PW-MPLS-MIB
- CISCO-IF-EXTENSION-MIB
- CISCO-IGMP-FILTER-MIB
- CISCO-IMAGE-MIB
- CISCO-IP-LOCAL-POOL-MIB
- CISCO-IPMROUTE-MIB
- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB
- CISCO-IP-TAP-MIB
- CISCO-IP-URPF-MIB
- CISCO-MVPN-MIB
- CISCO-NBAR-PROTOCOL-DISCOVERY-MIB
- CISCO-NETFLOW-MIB
- CISCO-NTP-MIB
- CISCO-OSPF-MIB (draft-ietf-ospf-mib-update-05)
- CISCO-OSPF-TRAP-MIB (draft-ietf-ospf-mib-update-05)
- CISCO-PIM-MIB
- CISCO-PING-MIB
- CISCO-PPPOE-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-QINQ-VLAN-MIB
- CISCO-RF-MIB
- CISCO-RTTMON-MIB
- CISCO-SESS-BORDER-CTRLR-CALL-STATS-MIB
- CISCO-SESS-BORDER-CTRLR-EVENT-MIB
- CISCO-SESS-BORDER-CTRLR-STATS-MIB
- CISCO-SONET-MIB
- CISCO-SYSLOG-MIB
- CISCO-TAP2-MIB
- CISCO-USER-CONNECTION-TAP-MIB
- CISCO-UNIFIED-FIREWALL-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VOIP-TAP-MIB
- CISCO-VPDN-MGMT-MIB
- DS1-MIB (RFC 2495)
- DS3-MIB (RFC 2496)
- ENTITY-MIB (RFC 4133)
- ENTITY-SENSOR-MIB (RFC 3433)
- ETHERLIKE-MIB (RFC 3635)
- ETHER-WIS
- EVENT-MIB (RFC 2981)
- EXPRESSION-MIB
- FRAME-RELAY-DTE-MIB (RFC1315-MIB)
- HC-ALARM-MIB
- IF-MIB (RFC 2863)
- IGMP-STD-MIB (RFC 2933)
MIBs Used in Cisco IOS XE 3S Releases

- IP-FORWARD-MIB (RFC 4292)
- IP-MIB (RFC 4293)
- IPMROUTE-STD-MIB (RFC 2932)
- MPLS-L3VPN-STD-MIB (RFC 4382)
- MPLS-LDP GENERIC-STD-MIB (RFC 3815)
- MPLS-LDP-STD-MIB (RFC 3815)
- MPLS-LSR-STD-MIB (RFC 3813)
- MPLS-TE-MIB
- MPLS-VPN-MIB
- MSDP-MIB
- NHRP-MIB
- NOTIFICATION-LOG-MIB (RFC 3014)
- OSPF-MIB (RFC 1850)
- OSPF-TRAP-MIB (RFC 1850)
- PIM-MIB (RFC 2934)
- RFC1213-MIB
- RMON-MIB (RFC 1757)
- RSVP-MIB
- SNMP-COMMUNITY-MIB (RFC 2576)
- SNMP-FRAMEWORK-MIB (RFC 2571)
- SNMP-MPD-MIB (RFC 2572)
- SNMP-NOTIFICATION-MIB (RFC 2573)
- SNMP-PROXY-MIB (RFC 2573)
- SNMP-TARGET-MIB (RFC 2573)
- SNMPv2-MIB (RFC 1907)
- SNMP-VIEW-BASED-ACM-MIB (RFC 2575)
- SONET-MIB (RFC 2558)
- TCP-MIB (RFC 4022)
- TUNNEL-MIB (RFC 4087)
- UDP-MIB (RFC 4113)

The Cisco ASR 1000 Series Routers support the following unverified and supported MIBs:

- ATM-FORUM-ADDR-REG-MIB
- ATM-FORUM-MIB
- CISCO-ATM-QOS-MIB

For information about the Cisco ASR 1000 Series Routers product implementation of the MIB protocol, see Cisco ASR 1000 Series Aggregation Services Routers MIB Specifications Guide at the following location:

Related Documentation for Cisco IOS XE 3S Releases

The following sections describe the documentation available for the Cisco ASR 1000 Series Routers and the Cisco ASR 903 Series Router for Cisco IOS XE 3S releases. These documents consist of hardware and software installation guides, system error messages, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on cisco.com.

This chapter contains the following sections:

- Platform-Specific Documents, page 479
- Cisco Feature Navigator, page 482
- Error Message Documentation for Cisco IOS XE 3S, page 482
- Cisco IOS XE 3S Software Documentation Set, page 483

Platform-Specific Documents

The following platform-specific documents are available for the Cisco ASR 1000 Series Routers on Cisco.com:

- Cisco ASR 903 Router Chassis Software Configuration Guide
  Describes the ISSU process on the Cisco ASR 903 Series Routers.

- Cisco ASR 1000 Series Aggregation Services Routers Documentation Roadmap
  Provides an online directory to quickly access publications for the Cisco ASR 1000 Series Routers.

- Cisco ASR 1002 Quick Start Guide
  Provides a summary of the hardware installation guide for the Cisco ASR 1002 Router.
- **Cisco ASR 1002-F Quick Start Guide**
  Provides a summary of the hardware installation guide for the Cisco ASR 1002-F Router.

- **Cisco ASR 1004 Quick Start Guide**
  Provides a summary of the hardware installation guide for the Cisco ASR 1004 Router.

- **Cisco ASR 1006 Quick Start Guide**
  Provides a summary of the hardware installation guide for the Cisco ASR 1006 Router.

- **Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide**
  Provides instructions for installing the Cisco ASR 1000 Series Routers and replacing or upgrading field-replaceable units (FRUs).

- **Cisco ASR 1000 Series Routers ROMmon Upgrade Guide**
  Contains procedures for upgrading the ROM monitor (ROMmon) on the Route Processors (RPs), Embedded Services Processors (ESP), and Shared Port Adapter Interface Processors (SIPs) on the Cisco ASR 1000 Series Routers.

- **Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide**
  Contains platform-specific information that does not fit logically into the train-based Cisco IOS configuration guides.

- **Cisco ASR 1000 Series Aggregation Services Routers Operations and Maintenance Guide**
  Provides operations and maintenance information that is specific to the Cisco ASR 1000 Series Routers.

- **Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide**
  Describes how to install the supported SIPs and SPAs on the Cisco ASR 1000 Series Routers and how to troubleshoot the installation.

- **Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide**
  Describes the configuration and troubleshooting of SPA interface processors (SIPs) and shared port adapters (SPAs) that are supported on the Cisco ASR 1000 Series Routers.

- **Cisco ASR 1000 Series Aggregation Services Routers MIB Specifications Guide**
  Describes the implementation of the Management Information Base (MIB) protocol on the Cisco ASR 1000 Series Routers.
- **Cisco ASR 1000 Embedded Services Processor 10G Non Crypto Capable New Feature**
  Provides restrictions and specific information related to the Cisco ASR 1000 Embedded Services Processor 10G Non Crypto Capable feature.
  

  

  Describes the commands used by the Cisco Unified Border Element (SP Edition) on the Cisco ASR 1000 Series Routers to configure, debug, and show statistics. The name Cisco Unified Border Element (SP Edition) replaces the Integrated Session Border Controller name. Introduces new commands supported in the unified model on Cisco Unified Border Element (SP Edition) for Cisco IOS XE Release 2.4.
  

- **Cisco IOS XE Integrated Session Border Controller Configuration Guide for the Cisco ASR 1000 Series Aggregation Services Routers**
  Describes the Integrated Session Border Controller (SBC) functions, features, and configuration tasks. A comprehensive guide for the Integrated Session Border Controller feature on the Cisco ASR 1000 Series Routers.
  

- **Cisco IOS Integrated Session Border Controller Command Reference**
  Describes the commands used by the Integrated Session Border Controller on the Cisco ASR 1000 Series Routers to configure, debug, and show statistics.
  

- **NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers matrix**
  Summarizes Network Address Translation (NAT) and Firewall Application Layer Gateway (ALG) feature support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1.0 and later releases.
  

- **Cisco IOS XE System Message Guide**
  Describes non-IOS messages specific to the Cisco ASR 1000 Series Routers.
  

- **Regulatory Compliance and Safety Information for the Cisco ASR 1000 Series Aggregation Services Routers**
  Provides international agency compliance, safety, and statutory information and translations for the safety warnings for the Cisco ASR 1000 Series Routers.
Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS, Catalyst OS, and Cisco IOS XE software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following location:

http://www.cisco.com/go/fn

Error Message Documentation for Cisco IOS XE 3S

Information about error messages for Cisco IOS XE Release 3S and later IOS XE releases can be found in the following locations:

- **Cisco IOS XE System Message Guide**
  
  Documents non-IOS messages specific to the Cisco ASR 1000 Series Routers.
  

- **Cisco IOS Release 12.2SB System Message Guide**
  
  Documents all messages available in Cisco IOS Release 12.2SB, which is a parent release for the Cisco IOS subpackage in Cisco IOS XE Release 2.
  

- **Cisco IOS Release 12.2SR System Message Guide**
  
  Documents all messages available in Cisco IOS Release 12.2SR, which is a parent release for the Cisco IOS subpackage in Cisco IOS XE Release 2.
  

- **Cisco IOS Error Message Decoder**
  
  The Cisco IOS Error Message Decoder is an online tool available to all registered Cisco.com users for researching and resolving error messages. This tool provides you with an explanation of the error message, a recommended action, and links to suggested online Cisco technical support resources.
  
  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi
Cisco IOS XE 3S Software Documentation Set

The Cisco IOS XE 3S software documentation set consists of Cisco IOS XE 3S configuration guides and Cisco IOS command references. The configuration guides are consolidated platform-independent configuration guides organized and presented by technology. There is one set of configuration guides for the Cisco IOS XE Release 2 release train and another for the Cisco IOS XE 3S release train. However, there is only one set of command references because they are platform independent—Cisco IOS command references support all Cisco platforms that are running any Cisco IOS or Cisco IOS XE software image.

Note  All content included in Cisco IOS XE Release 2 configuration guides is shared with and included in the Cisco IOS XE 3S configuration guides. As a result, some information for features introduced as part of Cisco IOS XE 3S may also be displayed in Cisco IOS XE Release 2 configuration guides.

Information in the configuration guides often includes related content that is shared across software releases and platforms. Some features referenced in these configuration guides may not be supported by Cisco IOS XE Release 2 and later releases or by the Cisco ASR 1000 Series Aggregation Services Routers. For the latest feature information and caveats in Cisco IOS XE Release 2 and later releases, see the Features, Important Notes, and Caveats section of these release notes.

Additionally, you can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on cisco.com is not required.
Open Source License Notices for Cisco IOS XE 3S Releases

This chapter provides information about open source license notices for Cisco IOS XE 3S Releases.

Open Source License Notices

For a listing of the license notices for open source software used in Cisco IOS XE 3S Releases, see the documents accessible from the License Information page at the following location:


Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2008–2013 Cisco Systems, Inc. All rights reserved.