Release Notes for Cisco ASR 1000 Series Aggregation Services Routers for Cisco IOS XE Release 2

Published: July 25, 2011
Revised: August 3, 2012, OL-16576-21

These release notes for the Cisco ASR 1000 Series Aggregation Services Routers support Cisco IOS XE Release 2.6.2 and earlier Release 2 releases. These release notes are updated as needed to describe new features, caveats, potential software deferrals, and related documents.

For a list of the software caveats that apply to Cisco IOS XE Release 2, see the "Caveats for Cisco IOS XE Release 2" section on page 167.

Cisco recommends that you view the field notices for this release to see if 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/customer/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.

Contents

These release notes describe the following topics:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

The Cisco ASR 1000 Series Aggregation Services Routers are the next generation Cisco midrange router products. The Cisco ASR 1000 Series Aggregation Services Routers use an innovative and powerful hardware processor technology known as the Cisco QuantumFlow Processor. The Cisco ASR 1000 Series Routers consist of three different routers: the Cisco ASR 1002 Router, the Cisco ASR 1004 Router, and the Cisco ASR 1006 Router.

- 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 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-rack-unit (RU), hardware-redundant chassis with two Embedded Services Processor (ESP) slots, two Route Processor (RP) slots, and three SIP slots.

For the single-route-processor Cisco ASR 1000 platforms, the Cisco ASR 1002 and Cisco ASR 1004, the Route Processor has a dual Cisco IOS Software option that allows these routers to use Cisco IOS software redundancy, Cisco high-availability features, Nonstop Forwarding (NSF), and In Service Software Upgrades (ISSUs). This option requires the Cisco ASR 1000 Series Route Processor to have 4 GB of DRAM memory.

The Cisco ASR 1006 Router supports fully redundant Route Processors that allow for full Route-Processor hardware redundancy, NSF, ISSU, and future Route-Processor service upgrades.

The Cisco ASR 1000 Series Routers run 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 Software is support for dual Cisco IOS software consolidated packages in a single Route Processor 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 6-RU chassis.

The Cisco ASR 1000 Series Routers target both enterprise and service provider applications and provide application-specific features for broadband subscriber aggregation and network application services with improved processing performance and high availability.

For information on new features and Cisco IOS commands supported by Cisco IOS XE Release 2, see the "New and Changed Information" section on page 33 and the "Related Documentation" section on page 158.

System Requirements

This section describes the system requirements for Cisco IOS XE Release 2 and includes the following sections:

Software Packaging on the Cisco ASR 1000 Series Routers

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

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

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

Note The sub-package functionality is intended for both upgrade and field support, and not all combinations of sub-packages are supported.

Each individual software sub-package can be upgraded individually, or all individual software sub-packages for a specific Cisco IOS XE consolidated package can be upgraded as part of a complete Cisco IOS XE consolidated package upgrade.

Importantly, IOS (the RPIOS individual software sub-package) is considered one of the individual software sub-packages that makes up the complete Cisco IOS XE consolidated package.

The following are the individual software sub-packages 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 sub-package: RPIOS-ipbase, RPIOS-ipbasek9, RPIOS-advipservices, RPIOS-advipservicesk9, RPIOS-adventservices, and RPIOS-adventservicesk9.

Note The RPIOS-advipservices and RPIOS-adventservices sub-packages are only available beginning with Cisco IOS XE Release 2.2.1 and later releases. These two sub-packages are not available with Cisco IOS XE Release 2.1.2 and earlier releases.

  - RPAccess: Provides components to manage enhanced router access functionality.

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

Note The Cisco ASR 1000 Series RP1 ADVANCED IP SERVICES W/O CRYPTO consolidated package is only available with Cisco IOS XE Release 2.2.1 through Cisco IOS XE Release 2.3.*x*. This consolidated package is not available with any other Cisco IOS XE Releases.

The Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES W/O CRYPTO consolidated package is only available beginning with Cisco IOS XE Release 2.2.1 and later releases. This consolidated package is not available with Cisco IOS XE Release 2.1.2 and earlier releases.

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
- Cisco ASR 1000 Series RP2 ADVANCED IP SERVICES W/O CRYPTO
- Cisco ASR 1000 Series RP2 ADVANCED ENTERPRISE SERVICES

- Cisco ASR 1000 Series RP2 ADVANCED ENTERPRISE SERVICES W/O CRYPTO

Note The RP2 consolidated packages are only available beginning with Cisco IOS XE Release 2.3.0 and later releases. The RP2 consolidated packages are not available with Cisco IOS XE Release 2.2.3 and earlier releases.

The Cisco ASR 1000 Series RP2 ADVANCED IP SERVICES W/O CRYPTO consolidated package is only available with Cisco IOS XE Release 2.3.0 through Cisco IOS XE Release 2.3.*x*. This consolidated package is not available with any other Cisco IOS XE Releases.

The individual software sub-packages within the consolidated packages cannot be downloaded from Cisco.com; only the Cisco IOS XE consolidated packages and optional sub-packages can be downloaded from Cisco.com. Users who want to run the router using individual software sub-packages must first download the consolidated package from Cisco.com and extract the individual software sub-packages from the consolidated package.

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

- For the RP1, the optional software sub-package available is the Cisco ASR 1000 Series RP1 WebEx Node (asr1000rp1-sipspawmak9.*version*.pkg)
- For the RP2, the optional software sub-package 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 sub-packages 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 RP*x* IP BASE, Cisco ASR 1000 Series RP*x* ADVANCED IP SERVICES, or Cisco ASR 1000 Series RPx ADVANCED ENTERPRISE SERVICES consolidated package. These optional software sub-packages 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 sub-package mode.

Note USB (or any other removable media) cannot be used to boot the system into sub-package mode.

For further information on the advantages and disadvantages of running individual sub-packages or a complete Cisco IOS XE consolidated package, and the process of extracting the individual sub-packages, see the following document:

Cisco ASR 1000 Series Aggregation Services Router Software Configuration Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/asrswcfg.html

Cisco IOS XE Software Package Compatibility for ISSU

When upgrading the Cisco IOS XE operating system software using the In Service Software Upgrade (ISSU) process, it is important to determine the compatibility of the upgraded software to your current software and hardware. The ISSU process allows software to be updated or otherwise modified while packet forwarding continues with minimal interruption.

Cisco IOS XE release compatibility using the ISSU process utilizes the SSO functionality to preserve state while software versions on the router differ, as during an upgrade. Most SSO-capable features in each Cisco IOS XE release are ISSU capable. ISSU is only supported if SSO is enabled in the configuration and the system is in a steady state (SSO ready state has been achieved). ISSU compatibility depends on the set of specific feature clients that are in use and whether they support ISSU. All ISSU upgrades include at least one IOS switchover operation. It is important to understand which features are in use and whether these features are ISSU compatible.

The Cisco ASR1006 Series Router is a hardware-redundant chassis. The hardware-redundant chassis has two ESP linecards and two RPs which exchange state using hardware links. The Cisco ASR1002 and ASR1004 Series Routers are not hardware redundant, but are software-redundancy capable. The non-redundant chassis has a single RP and a single ESP, but allows the operation of up to two IOS processes on the single RP to exchange states locally.

- Non-hardware-redundant chassis models (such as the Cisco ASR 1002 Router and Cisco ASR 1004 Router)—Supports ISSU only if the router is running in subpackage mode.
- Hardware-redundant chassis models (such as the Cisco ASR 1006 Router)—Supports ISSU when the router is running in sub-package mode or in consolidated package mode.

For a complete discussion about the ISSU upgrade process on the Cisco ASR 1000 Series Routers, including prerequisites and restrictions, see the "In Service Software Upgrade (ISSU)" chapter of the *Cisco ASR 1000 Series Aggregation Services Software Configuration Guide.*

Compatibility Support Policy

Rebuilds of a specific Cisco IOS XE release are intended to be fully ISSU and SSO capable for supported features between any two image pairings, however compatibility is not guaranteed for all releases. It is expected that rebuilds between release versions are compatible within a reasonable time frame.

Support for Cisco IOS XE Rebuilds

The support policy for version rebuilds is as follows:

- The immediate prior rebuild for the version is expected to be SSO and ISSU compatible with a new released rebuild of that version.
- A newly released rebuild is expected to be SSO and ISSU compatible with the current rebuild for the previous two versions.

As an example, a rebuild Y of version X is version XY. For rebuilds on the two previous versions of X, X-1 and X-2, it is expected that XY will be compatible with those versions.

Support for Special Cisco IOS XE Releases

Certain special Cisco IOS XE software releases may be made from time to time. These releases are not specified in this document and any supported SSO or ISSU interoperability must be determined on a case by case basis.

Cisco IOS XE Release Compatibility Tables

The ISSU compatibility tables in this section provide information about release pairs that are compatible and those that are not compatible for Cisco ASR1000 Series Routers. You can use this information to determine the impact of a Route Processor (RP) or Embedded Service Processor (ESP) switchover when the router is running a mixed combination of software as occurs during the whole-node ISSU procedures.

Non-SSO-capable features and non-ISSU-capable features are not included in the ISSU compatibility tables since these features lose state on any Cisco IOS XE switchover—RP switchover in the case of hardware-redundant chassis and software switchover on software-redundant chassis.

Discussion of Table Fields

In the ISSU compatibility tables, the following information is provided:

- SSO

  A Cisco IOS XE release stating :SSO" for all supported SSO-capable features is fully compatible for upgrades using ISSU, even if some of the SSO-capable features are not ISSU capable. Two different versions of the software are denoted as supporting SSO if they are able to reach an SSO state when run simultaneously, regardless of the impact on specific features.

- SSO Tested

  A Cisco IOS XE release stating "SSO Tested" indicates that the two releases are fully tested and supported as interoperable and will retain state across a switchover. ISSU upgrades between the releases are supported.

- SSO via <*release*>

  A Cisco IOS XE release stating "SSO via <*release*>" indicates that the two releases are not interoperable and must not be run simultaneously (must not be run at the same time on the two RPs of a hardware redundant chassis and must not be co-installed as subpackages on any chassis). However, an SSO path exists using the intermediate release that is specified.

- Limited

  A Cisco IOS XE release stating "Limited" indicates that the two releases have interoperability limitations. On the Cisco ASR1002 and Cisco ASR1004 routers. ISSU upgrade and downgrade are not supported. Instead you can perform a sub-package software upgrade. This process requires a RP reload.

The tables in the following sections list the compatibility of Cisco IOS XE software releases:

- ISSU Compatibility for Cisco IOS XE 2.1-Based Releases, page 8
- ISSU Compatibility for Cisco IOS XE 2.2-Based Releases, page 9
- ISSU Compatibility for Cisco IOS XE 2.3-Based Releases, page 12
- ISSU Compatibility for Cisco IOS XE 2.4-Based Releases, page 14
- ISSU Compatibility for Cisco IOS XE 2.5-Based Releases, page 17
- ISSU Compatibility for Cisco IOS XE 2.6-Based Releases, page 18

Note The ISSU compatibility tables use the following conventions:

- The software version numbers are given first as the Cisco IOS XE release version number followed by the bundled Cisco IOS release number.
- For descriptions of the table fields, see the "Discussion of Table Fields" section on page 7.

Caution For upgrading deployed releases prior to Cisco IOS XE 2.1.2, refer to the appropriate configuration guide. Some adjustments to the configuration procedure may be necessary due to changes in the installation command syntax. See *Cisco IOS XE Software Configuration Guides*.

ISSU Compatibility for Cisco IOS XE 2.1-Based Releases

Note When not labeled, the compatibility information shown in Table 1-1 applies to all platforms based on the package mode supported for ISSU on that platform. In some cases, compatibility information varies by platform and is indicated in the table.

Note Cisco ASR1002 and Cisco ASR1004 routers do not support ISSU upgrade and downgrade due to lack of hardware redundancy and the requirement to reboot the RP. However, the sub-package software upgrade and downgrade is supported only if the router is running in sub-package mode in order to minimize interruption to service.

Table 1-1 Cisco IOS XE Compatibility for the Cisco ASR 1000 Series Routers

Deployed Cisco IOS XE Release	Target Release: Cisco IOS XE 2.1.0 12.2(33)XNA	Target Release: Cisco IOS XE 2.1.1 12.2(33)XNA1	Target Release: Cisco IOS XE 2.1.2 12.2(33)XNA2
Cisco IOS XE 2.1.0 12.2(33)XNA	—	SSO Tested[1]	SSO Tested[1]
Cisco IOS XE 2.1.1 12.2(33)XNA1	SSO Tested[1]	—	SSO Tested
Cisco IOS XE 2.1.2 12.2(33)XNA2	SSO Tested[1]	SSO Tested	—
Cisco IOS XE 2.2.1 12.2(33)XNB1	**Cisco ASR 1006 Router** SSO via 2.1.2[1] **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited.	**Cisco ASR 1006 Router** SSO via 2.1.2 **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited	**Cisco ASR 1006 Router** SSO Tested **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited

Table 1-1 Cisco IOS XE Compatibility for the Cisco ASR 1000 Series Routers (continued)

Deployed Cisco IOS XE Release	Target Release: Cisco IOS XE 2.1.0 12.2(33)XNA	Target Release: Cisco IOS XE 2.1.1 12.2(33)XNA1	Target Release: Cisco IOS XE 2.1.2 12.2(33)XNA2
Cisco IOS XE 2.2.2 12.2(33)XNB2	SSO via 2.1.2[1]	SSO via 2.1.2	Limited[2 and 3]
Cisco IOS XE 2.2.3 12.2(33)XNB3	SSO via 2.1.2	SSO via 2.1.2	Limited[2 and 3]
Cisco IOS XE 2.3.0 12.2(33)XNC	SSO via 2.1.2	SSO via 2.1.2	Limited[2 and 3]
Cisco IOS XE 2.3.1 12.2(33)XNC1	SSO via 2.1.2	SSO via 2.1.2	Limited[2 and 3]
Cisco IOS XE 2.3.2 12.2(33)XNC2	SSO via 2.1.2	SSO via 2.1.2	Limited[2 and 3]

1. For Cisco ASR 1006 Router, some ESP-maintained session state may be lost when ESPs of different versions interoperate. This affects primarily stateful firewall and network address translation functions implemented by the ESPs.
2. For Cisco ASR 1006 Router, downgrade may fail depending on the features that are configured.
3. For Cisco ASR 1002 Router and Cisco ASR 1004 Routers, the Cisco IOS XE software on the standby RP may spontaneously restart creating a core dump file when **issu loadversion** (**issu** command set) or **request platform software package install** (**request platform** command set) is used to simultaneously install the RP packages other than the base package (as specified by the {**rpcontrol,rpaccess,rpios**} portion of the filename specification). The Cisco IOS XE software on the standby RP will recover after this event.

ISSU Compatibility for Cisco IOS XE 2.2-Based Releases

Note When not labeled, the compatibility information shown in Table 1-2 applies to all platforms based on the package mode supported for ISSU on that platform. In some cases, compatibility information varies by platform and is indicated in the table.

Note Cisco ASR1002 and Cisco ASR1004 routers do not support ISSU upgrade and downgrade due to lack of hardware redundancy and the requirement to reboot the RP. However, the sub-package software upgrade and downgrade is supported only if the router is running in sub-package mode in order to minimize interruption to service.

Note Cisco IOS XE 2.4.2t does not support ISSU upgrade and downgrade.

Table 1-2 Cisco IOS XE Compatibility for the Cisco ASR 1000 Series Routers

Deployed Cisco IOS XE Release	Target Release: Cisco IOS XE 2.2.1 12.2(33)XNB1	Target Release: Cisco IOS XE 2.2.2 12.2(33)XNB2	Target Release: Cisco IOS XE 2.2.3 12.2(33)XNB3
Cisco IOS XE 2.1.0 12.2(33)XNA	SSO via 2.1.2[1]	SSO via 2.1.2	SSO via 2.1.2
Cisco IOS XE 2.1.1 12.2(33)XNA1	SSO via 2.1.2	SSO via 2.1.2	SSO via 2.1.2
Cisco IOS XE 2.1.2 12.2(33)XNA2	SSO Tested	SSO Tested	SSO Tested[2 and 3]
Cisco IOS XE 2.2.1 12.2(33)XNB1	—	SSO Tested	SSO Tested
Cisco IOS XE 2.2.2 12.2(33)XNB2	SSO Tested	—	SSO Tested
Cisco IOS XE 2.2.3 12.2(33)XNB3	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited[4]	SSO Tested	—
Cisco IOS XE 2.3.0 12.2(33)XNC	Limited[4 and 5]	SSO Tested	SSO Tested
Cisco IOS XE 2.3.1 12.2(33)XNC1	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	SSO Tested
Cisco IOS XE 2.3.2 12.2(33)XNC2	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	SSO Tested
Cisco IOS XE 2.4.0 12.2(33)XND	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	SSO Tested

Table 1-2 Cisco IOS XE Compatibility for the Cisco ASR 1000 Series Routers (continued)

Deployed Cisco IOS XE Release	Target Release: Cisco IOS XE 2.2.1 12.2(33)XNB1	Target Release: Cisco IOS XE 2.2.2 12.2(33)XNB2	Target Release: Cisco IOS XE 2.2.3 12.2(33)XNB3
Cisco IOS XE 2.4.1 12.2(33)XND1	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	SSO[6]
Cisco IOS XE 2.4.2 12.2(33)XND2	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	SSO Tested[7]
Cisco IOS XE 2.4.3 12.2(33)XND3	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	SSO
Cisco IOS XE 2.4.4 12.2(33)XND4	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** Limited SSO via 2.2.3	SSO

1. For the Cisco ASR 1006 Router, some ESP-maintained session state may be lost when ESPs of different versions interoperate. This affects primarily stateful firewall and network address translation functions implemented by the ESPs.
2. For the Cisco ASR 1006 Router, use of new features in the uprev release may be limited after ISSU. To correct this issue, perform an additional redundancy force-switchover after completing all steps of the ISSU procedure and after the device has reached SSO. Alternatively, a chassis reload also addresses the issue.
3. For the Cisco ASR 1002 Router and Cisco ASR 1004 Routers, when ISSU is used to upgrade router software, new features available in the new version are configurable as soon as the RP software portion of the update has been completed for both active and standby IOS. New features will be fully reflected in the operation of the router once the linecard images are also updated. Under some circumstances, the new features may not be available until after the final step of the Cisco ASR1002 and Cisco ASR1004 ISSU procedure is performed (chassis reload).
4. For the Cisco ASR 1002 Router and Cisco ASR 1004 Routers, the Cisco IOS XE software on the standby RP may spontaneously restart creating a core dump file when **issu loadversion** (**issu** command set) or **request platform software package install** (**request platform** command set) is used to simultaneously install the RP packages other than the base package (as specified by the {rpcontrol,rpaccess,rpios} portion of the filename specification). The Cisco IOS XE software on the standby RP will recover after this event.
5. For the Cisco ASR 1006 Router, downgrade may fail depending on the features that are configured.
6. After ISSU procedure, you might need to run an additional switchover to ensure R0 is active.
7. The forwarding processor (FP) remains in “init” state during ISSU sub-package procedure when broadband QoS is configured. The workaround is to recreate some broadband sessions, tear down all sessions, or unconfigure QoS queueing feature on the broadband sessions and then reload the FP. For more information, refer to CSCsz09462 in the Bug Toolkit.

ISSU Compatibility for Cisco IOS XE 2.3-Based Releases

Note When not labeled, the compatibility information shown in Table 1-3 applies to all platforms based on the package mode supported for ISSU on that platform. In some cases, compatibility information varies by platform and is indicated in the table.

Note Cisco ASR1002 and Cisco ASR1004 routers do not support ISSU upgrade and downgrade due to lack of hardware redundancy and the requirement to reboot the RP. However, the sub-package software upgrade and downgrade is supported only if the router is running in sub-package mode in order to minimize interruption to service.

Note Cisco IOS XE 2.4.2t does not support ISSU upgrade and downgrade.

Table 1-3 Cisco IOS XE Compatibility for the Cisco ASR 1000 Series Routers

Deployed Cisco IOS XE Release	Target Release: Cisco IOS XE 2.3.0 12.2(33)XNC	Target Release: Cisco IOS XE 2.3.1 12.2(33)XNC1	Target Release: Cisco IOS XE 2.3.2 12.2(33)XNC2
Cisco IOS XE 2.1.0 12.2(33)XNA	SSO via 2.1.2	SSO via 2.1.2	SSO via 2.1.2
Cisco IOS XE 2.1.1 12.2(33)XNA1	SSO via 2.1.2	SSO via 2.1.2	SSO via 2.1.2
Cisco IOS XE 2.1.2 12.2(33)XNA2	**Cisco ASR 1006 Router** SSO Tested[1] **Cisco ASR 1002 and Cisco ASR 1004 Routers** SSO via 2.2.2	**Cisco ASR 1006 Router** SSO Tested[1] **Cisco ASR 1002 and Cisco ASR 1004 Routers** SSO via 2.2.2	**Cisco ASR 1006 Router** SSO Tested[1] **Cisco ASR 1002 and Cisco ASR 1004 Routers** SSO via 2.2.2
Cisco IOS XE 2.2.1 12.2(33)XNB1	**Cisco ASR 1006 Router** SSO Tested[1] **Cisco ASR 1002 and Cisco ASR 1004 Routers** SSO via 2.2.2	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** SSO via 2.2.3	SSO
Cisco IOS XE 2.2.2 12.2(33)XNB2	SSO Tested[1]	**Cisco ASR 1006 Router** SSO Tested **Cisco ASR 1002 and Cisco ASR 1004 Routers** SSO via 2.2.3	SSO Tested
Cisco IOS XE 2.2.3 12.2(33)XNB3	SSO Tested[1]	SSO Tested	SSO Tested

Table 1-3 Cisco IOS XE Compatibility for the Cisco ASR 1000 Series Routers (continued)

Deployed Cisco IOS XE Release	Target Release: Cisco IOS XE 2.3.0 12.2(33)XNC	Target Release: Cisco IOS XE 2.3.1 12.2(33)XNC1	Target Release: Cisco IOS XE 2.3.2 12.2(33)XNC2
Cisco IOS XE 2.3.0 12.2(33)XNC	—	SSO Tested	SSO Tested
Cisco IOS XE 2.3.1 12.2(33)XNC1	SSO Tested	—	SSO Tested
Cisco IOS XE 2.3.2 12.2(33)XNC2	SSO Tested	SSO Tested	—
Cisco IOS XE 2.4.0 12.2(33)XND	SSO	SSO Tested	SSO Tested
Cisco IOS XE 2.4.1 12.2(33)XND1	SSO	SSO	SSO Tested
Cisco IOS XE 2.4.2 12.2(33)XND2	SSO	SSO	SSO Tested
Cisco IOS XE 2.4.3 12.2(33)XND3	SSO	SSO	SSO Tested
Cisco IOS XE 2.4.4 12.2(33)XND4	SSO	SSO	SSO Tested[2]
Cisco IOS XE 2.5.0[3] 12.2(33)XNE	SSO	SSO	SSO Tested
Cisco IOS XE 2.5.1 12.2(33)XNE1	SSO[4]	SSO[4]	SSO Tested[4]
Cisco IOS XE 2.5.2 12.2(33)XNE2	SSO[4]	SSO[4]	SSO Tested[4]

1. For the Cisco ASR 1006 Router, use of new features in the uprev release may be limited after ISSU. To correct this issue, perform an additional redundancy force-switchover after completing all steps of the ISSU procedure and after the device has reached SSO. Alternatively, a chassis reload also addresses the issue.
2. A loopback interface Outbound Cache Entry (OCE) may be lost after an RP failover.
3. For ATM SPAs on the Cisco ASR1000 Series Routers, ISSU from releases prior to Cisco IOS XE Release 2.5.0 to Cisco IOS XE Release 2.5.0, or from Cisco IOS XE Release 2.5.0 to a release prior to Cisco IOS XE Release 2.5.0, is not supported. If you want to perform ISSU in this environment, you must first remove the configuration from the ATM SPAs on the router, and then shut down the SPAs using the **shutdown** command prior to running the ISSU process.
4. PPP sessions requiring AAA authentication and authorization will not be synchronized to standby after ISSU upgrade procedure. This applies to scenarios where the Cisco ASR 1000 Series Router is acting as a PPP Termination and Aggregation (PTA) or L2TP network server (LNS) terminating PPP sessions.

ISSU Compatibility for Cisco IOS XE 2.4-Based Releases

Note When not labeled, the compatibility information shown in Table 1-4 applies to all platforms based on the package mode supported for ISSU on that platform. In some cases, compatibility information varies by platform and is indicated in the table.

Note Cisco ASR1002 and Cisco ASR1004 routers do not support ISSU upgrade and downgrade due to lack of hardware redundancy and the requirement to reboot the RP. However, the sub-package software upgrade and downgrade is supported only if the router is running in sub-package mode in order to minimize interruption to service.

Note Cisco IOS XE 2.4.2t does not support ISSU upgrade and downgrade.

Table 1-4 Cisco IOS XE Compatibility for the Cisco ASR 1000 Series Routers

Deployed Cisco IOS XE Release	Target Release: Cisco IOS XE 2.4.0 12.2(33)XND	Target Release: Cisco IOS XE 2.4.1 12.2(33)XND1	Target Release: Cisco IOS XE 2.4.2 12.2(33)XND2	Target Release: Cisco IOS XE 2.4.3 12.2(33)XND3	Target Release: Cisco IOS XE 2.4.4 12.2(33)XND4
Cisco IOS XE 2.2.1 12.2(33)XNB1	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** SSO via 2.2.3	SSO	SSO	SSO	SSO
Cisco IOS XE 2.2.2 12.2(33)XNB2	**Cisco ASR 1006 Router** SSO **Cisco ASR 1002 and Cisco ASR 1004 Routers** SSO via 2.2.3	SSO	SSO	SSO	SSO
Cisco IOS XE 2.2.3 12.2(33)XNB3	SSO Tested	SSO Tested	SSO Tested	SSO	SSO
Cisco IOS XE 2.3.0 12.2(33)XNC	SSO	SSO	SSO	SSO	SSO

Table 1-4 Cisco IOS XE Compatibility for the Cisco ASR 1000 Series Routers (continued)

Deployed Cisco IOS XE Release	Target Release: Cisco IOS XE 2.4.0 12.2(33)XND	Target Release: Cisco IOS XE 2.4.1 12.2(33)XND1	Target Release: Cisco IOS XE 2.4.2 12.2(33)XND2	Target Release: Cisco IOS XE 2.4.3 12.2(33)XND3	Target Release: Cisco IOS XE 2.4.4 12.2(33)XND4
Cisco IOS XE 2.3.1 12.2(33)XNC1	SSO Tested	SSO	SSO	SSO	SSO
Cisco IOS XE 2.3.2 12.2(33)XNC2	SSO Tested	SSO Tested	SSO Tested	SSO Tested	SSO Tested[1]
Cisco IOS XE 2.4.0 12.2(33)XND	—	SSO Tested	SSO Tested[2]	SSO	SSO
Cisco IOS XE 2.4.1 12.2(33)XND1	SSO Tested	—	SSO Tested	SSO	SSO
Cisco IOS XE 2.4.2 12.2(33)XND2	SSO Tested[2]	SSO Tested	—	SSO Tested	SSO Tested[1]
Cisco IOS XE 2.4.3 12.2(33)XND3	SSO	SSO	SSO Tested	—	SSO Tested[1]
Cisco IOS XE 2.4.4 12.2(33)XND4	SSO	SSO Tested[1]	SSO Tested[1]	SSO Tested[1]	—
Cisco IOS XE 2.5.0[3] 12.2(33)XNE	SSO	SSO	SSO Tested	SSO	SSO
Cisco IOS XE 2.5.1 12.2(33)XNE1	SSO[4]	SSO[4]	SSO Tested[4]	SSO Tested[4]	SSO[4]
Cisco IOS XE 2.5.2 12.2(33)XNE2	SSO[4]	SSO[4]	SSO Tested[4]	SSO Tested[4]	SSO Tested[1,4]
Cisco IOS XE 2.6.0 12.2(33)XNF	SSO[4]	SSO[4]	SSO Tested[4]	SSO Tested[4]	SSO[4]

Table 1-4 Cisco IOS XE Compatibility for the Cisco ASR 1000 Series Routers (continued)

Deployed Cisco IOS XE Release	Target Release: Cisco IOS XE 2.4.0 12.2(33)XND	Target Release: Cisco IOS XE 2.4.1 12.2(33)XND1	Target Release: Cisco IOS XE 2.4.2 12.2(33)XND2	Target Release: Cisco IOS XE 2.4.3 12.2(33)XND3	Target Release: Cisco IOS XE 2.4.4 12.2(33)XND4
Cisco IOS XE 2.6.1 12.2(33)XNF1	SSO[4]	SSO[4]	SSO[4]	SSO Tested[4]	SSO Tested[4]
Cisco IOS XE 2.6.2 12.2(33)XNF2	SSO[4]	SSO[4]	SSO[4]	SSO[4]	SSO Tested[1,4]

1. A loopback interface Outbound Cache Entry (OCE) may be lost after an RP failover.
2. The Cisco IOS XE software might fail during the ISSU process while the network clock is configured. For more information about the conditions and workaround, refer to CSCsz12394 in the Bug Toolkit.
3. For ATM SPAs on the Cisco ASR1000 Series Routers, ISSU from releases prior to Cisco IOS XE Release 2.5.0 to Cisco IOS XE Release 2.5.0, or from Cisco IOS XE Release 2.5.0 to a release prior to Cisco IOS XE Release 2.5.0, is not supported. If you want to perform ISSU in this environment, you must first remove the configuration from the ATM SPAs on the router, and then shut down the SPAs using the **shutdown** command prior to running the ISSU process.
4. PPP sessions requiring AAA authentication and authorization will not be synchronized to standby after ISSU upgrade procedure. This applies to scenarios where the Cisco ASR 1000 Series Router is acting as a PPP Termination and Aggregation (PTA) or L2TP network server (LNS) terminating PPP sessions.

ISSU Compatibility for Cisco IOS XE 2.5-Based Releases

Note For ATM SPAs on the Cisco ASR1000 Series Routers, ISSU from releases prior to Cisco IOS XE Release 2.5.0 to Cisco IOS XE Release 2.5.0, or from Cisco IOS XE Release 2.5.0 to a release prior to Cisco IOS XE Release 2.5.0, is not supported. If you want to perform ISSU in this environment, you must first remove the configuration from the ATM SPAs on the router, and then shut down the SPAs using the **shutdown** command prior to running the ISSU process.

Note Cisco ASR1002 and Cisco ASR1004 routers do not support ISSU upgrade and downgrade due to lack of hardware redundancy and the requirement to reboot the RP. However, the sub-package software upgrade and downgrade is supported only if the router is running in sub-package mode in order to minimize interruption to service.

Note Cisco IOS XE 2.4.2t does not support ISSU upgrade and downgrade.

Table 1-5 Cisco IOS XE Compatibility for the Cisco ASR 1000 Series Routers

Deployed Cisco IOS XE Release	Target Release: Cisco IOS XE 2.5.0[1] 12.2(33)XNE	Target Release: Cisco IOS XE 2.5.1 12.2(33)XNE1	Target Release: Cisco IOS XE 2.5.2 12.2(33)XNE2
Cisco IOS XE 2.3.0 12.2(33)XNC	SSO	SSO	SSO
Cisco IOS XE 2.3.1 12.2(33)XNC1	SSO	SSO	SSO
Cisco IOS XE 2.3.2 12.2(33)XNC2	SSO Tested	SSO Tested	SSO Tested
Cisco IOS XE 2.4.0 12.2(33)XND	SSO	SSO	SSO
Cisco IOS XE 2.4.1 12.2(33)XND1	SSO	SSO	SSO
Cisco IOS XE 2.4.2 12.2(33)XND2	SSO Tested[2]	SSO Tested[2]	SSO[2]
Cisco IOS XE 2.4.3 12.2(33)XND3	SSO	SSO	SSO Tested
Cisco IOS XE 2.4.4 12.2(33)XND4	SSO[2]	SSO[2]	SSO Tested[2,3]

Table 1-5 Cisco IOS XE Compatibility for the Cisco ASR 1000 Series Routers (continued)

Deployed Cisco IOS XE Release	Target Release: Cisco IOS XE 2.5.0[1] 12.2(33)XNE	Target Release: Cisco IOS XE 2.5.1 12.2(33)XNE1	Target Release: Cisco IOS XE 2.5.2 12.2(33)XNE2
Cisco IOS XE 2.5.0[1] 12.2(33)XNE	—	SSO Tested	SSO Tested
Cisco IOS XE 2.5.1 12.2(33)XNE1	SSO Tested	—	SSO Tested
Cisco IOS XE 2.5.2 12.2(33)XNE2	SSO Tested	SSO Tested	—
Cisco IOS XE 2.6.0 12.2(33)XNF	SSO	SSO Tested	SSO Tested
Cisco IOS XE 2.6.1 12.2(33)XNF1	SSO	SSO	SSO Tested
Cisco IOS XE 2.6.2 12.2(33)XNF2	SSO	SSO	SSO Tested[3]

1. For ATM SPAs on the Cisco ASR1000 Series Routers, ISSU from releases prior to Cisco IOS XE Release 2.5.0 to Cisco IOS XE Release 2.5.0, or from Cisco IOS XE Release 2.5.0 to a release prior to Cisco IOS XE Release 2.5.0, is not supported. If you want to perform ISSU in this environment, you must first remove the configuration from the ATM SPAs on the router, and then shut down the SPAs using the **shutdown** command prior to running the ISSU process.
2. PPP sessions requiring AAA authentication and authorization will not be synchronized to standby after ISSU upgrade procedure. This applies to scenarios where the Cisco ASR 1000 Series Router is acting as a PPP Termination and Aggregation (PTA) or L2TP network server (LNS) terminating PPP sessions.
3. A loopback interface Outbound Cache Entry (OCE) may be lost after an RP failover.

ISSU Compatibility for Cisco IOS XE 2.6-Based Releases

Note Cisco ASR1002 and Cisco ASR1004 routers do not support ISSU upgrade and downgrade due to lack of hardware redundancy and the requirement to reboot the RP. However, the sub-package software upgrade and downgrade is supported only if the router is running in sub-package mode in order to minimize interruption to service.

Note Cisco IOS XE 2.4.2t does not support ISSU upgrade and downgrade.

Table 1-6 Cisco IOS XE Compatibility for the Cisco ASR 1000 Series Routers

Deployed Cisco IOS XE Release	Target Release: Cisco IOS XE 2.6.0 12.2(33)XNF	Target Release: Cisco IOS XE 2.6.1 12.2(33)XNF1	Target Release: Cisco IOS XE 2.6.2 12.2(33)XNF2
Cisco IOS XE 2.4.0 12.2(33)XND	SSO[1]	SSO[1]	SSO[1]
Cisco IOS XE 2.4.1 12.2(33)XND1	SSO[1]	SSO[1]	SSO[1]
Cisco IOS XE 2.4.2 12.2(33)XND2	SSO Tested[1]	SSO[1]	SSO[1]
Cisco IOS XE 2.4.3 12.2(33)XND3	SSO Tested[1]	SSO Tested[1]	SSO[1]
Cisco IOS XE 2.4.4 12.2(33)XND4	SSO[1]	SSO Tested[1]	SSO Tested[1]
Cisco IOS XE 2.5.0 12.2(33)XNE	SSO	SSO	SSO
Cisco IOS XE 2.5.1 12.2(33)XNE1	SSO Tested	SSO	SSO
Cisco IOS XE 2.5.2 12.2(33)XNE2	SSO Tested	SSO Tested	SSO Tested
Cisco IOS XE 2.6.0 12.2(33)XNF	—	SSO Tested	SSO Tested
Cisco IOS XE 2.6.1 12.2(33)XNF1	SSO Tested	—	SSO Tested
Cisco IOS XE 2.6.2 12.2(33)XNF1	SSO Tested	SSO Tested	SSO Tested

1. PPP sessions requiring AAA authentication and authorization will not be synchronized to standby after ISSU upgrade procedure. This applies to scenarios where the Cisco ASR 1000 Series Router is acting as a PPP Termination and Aggregation (PTA) or L2TP network server (LNS) terminating PPP sessions.

RP Memory Recommendations

The Cisco IOS XE images and packages available vary based on the Route Processor (RP) installed in the system: RP1 or RP2.

- Table 7 describes the RP1 consolidated package images, their individual software sub-package contents, and their memory recommendations.

- Table 9 describes the RP1 optional sub-package images and their memory recommendations.
- Table 9 describes the RP2 consolidated package images, their individual software sub-package contents, and their memory recommendations.
- Table 10 describes the RP2 optional sub-package images and their memory recommendations.

Each Cisco IOS XE image also contains two provisioning files: asr1000rp*x*-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 image and then used to run the router. Either provisioning file can be used.

Note No In Service Software Upgrade (ISSU) is possible between different image types.

Table 7 RP1 Memory Recommendations for the Cisco ASR 1000 Series Routers Consolidated Package Images

Platforms	Image Name	Software Image	Individual Sub-Package Contents	DRAM Memory
Cisco ASR 1002 Router **Cisco ASR 1004 Router** **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP1 IP BASE W/O CRYPTO	asr1000rp1-ipbase.*version*.bin	asr1000rp1-rpbase.*version*.pkg	4GB (for Cisco ASR 1002 Router) 2GB-4GB (for Cisco ASR 1004 and Cisco ASR 1006 routers)
			asr1000rp1-rpcontrol.*version*.pkg	
			asr1000rp1-rpaccess.*version*.pkg	
			asr1000rp1-rpios-ipbase.*version*.pkg	
			asr1000rp1-espbase.*version.pkg*	
			asr1000rp1-sipbase.*version*.pkg	
			asr1000rp1-sipspa.*version*.pkg	
			asr1000rp1-packages-ipbase.*version*.conf	
			packages.conf	
Cisco ASR 1002 Router **Cisco ASR 1004 Router** **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP1 IP BASE	asr1000rp1-ipbasek9.*version*.bin	asr1000rp1-rpbase.*version*.pkg	4GB (for Cisco ASR 1002 Router) 2GB-4GB (for Cisco ASR 1004 and Cisco ASR 1006 routers)
			asr1000rp1-rpcontrol.*version*.pkg	
			asr1000rp1-rpaccess.*version*.pkg	
			asr1000rp1-rpios-ipbasek9.*version*.pkg	
			asr1000rp1-espbase.*version*.pkg	
			asr1000rp1-sipbase.*version*.pkg	
			asr1000rp1-sipspa.*version*.pkg	
			asr1000rp1-packages-ipbasek9.*version*.conf	
			packages.conf	

Table 7 RP1 Memory Recommendations for the Cisco ASR 1000 Series Routers Consolidated Package Images

Platforms	Image Name	Software Image	Individual Sub-Package Contents	DRAM Memory
Cisco ASR 1002 Router **Cisco ASR 1004 Router** **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP1 ADVANCED IP SERVICES W/O CRYPTO[1]	asr1000rp1-advipservices.*version*.bin	asr1000rp1-rpbase.*version*.pkg	4GB (for Cisco ASR 1002 Router) 2GB-4GB (for Cisco ASR 1004 and Cisco ASR 1006 routers)
			asr1000rp1-rpcontrol.*version*.pkg	
			asr1000rp1-rpaccess.*version*.pkg	
			asr1000rp1-rpios-advipservices.*version*.pkg	
			asr1000rp1-espbase.*version*.pkg	
			asr1000rp1-sipbase.*version*.pkg	
			asr1000rp1-sipspa.*version*.pkg	
			asr1000rp1-packages-advipservices.*version*.conf	
			packages.conf	
Cisco ASR 1002 Router **Cisco ASR 1004 Router** **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP1 ADVANCED IP SERVICES	asr1000rp1-advipservicesk9.*version*.bin	asr1000rp1-rpbase.*version*.pkg	4GB (for Cisco ASR 1002 Router) 2GB-4GB (for Cisco ASR 1004 and Cisco ASR 1006 routers)
			asr1000rp1-rpcontrol.*version*.pkg	
			asr1000rp1-rpaccess.*version*.pkg	
			asr1000rp1-rpios-ipbasek9.*version*.pkg	
			asr1000rp1-espbase.*version*.pkg	
			asr1000rp1-sipbase.*version*.pkg	
			asr1000rp1-sipspa.*version*.pkg	
			asr1000rp1-packages-advipservicesk9.*version*.conf	
			packages.conf	
Cisco ASR 1002 Router **Cisco ASR 1004 Router** **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES W/O CRYPTO[2]	asr1000rp1-adventservices.*version*.bin	asr1000rp1-rpbase.*version*.pkg	4GB (for Cisco ASR 1002 Router) 2GB-4GB (for Cisco ASR 1004 and Cisco ASR 1006 routers)
			asr1000rp1-rpcontrol.*version*.pkg	
			asr1000rp1-rpaccess.*version*.pkg	
			asr1000rp1-rpios-adventservices.*version*.pkg	
			asr1000rp1-espbase.*version*.pkg	
			asr1000rp1-sipbase.*version*.pkg	
			asr1000rp1-sipspa.*version*.pkg	
			asr1000rp1-packages-adventservices.*version*.conf	
			packages.conf	

Table 7 RP1 Memory Recommendations for the Cisco ASR 1000 Series Routers Consolidated Package Images

Platforms	Image Name	Software Image	Individual Sub-Package Contents	DRAM Memory
Cisco ASR 1002 Router **Cisco ASR 1004 Router** **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	asr1000rp1-adventservicesk9.*version*.bin	asr1000rp1-rpbase.*version*.pkg	4GB (for Cisco ASR 1002 Router) 2GB-4GB (for Cisco ASR 1004 and Cisco ASR 1006 routers)
			asr1000rp1-rpcontrol.*version*.pkg	
			asr1000rp1-rpaccess.*version*.pkg	
			asr1000rp1-rpios-adventservicesk9.*version*.pkg	
			asr1000rp1-espbase.*version*.pkg	
			asr1000rp1-sipbase.*version*.pkg	
			asr1000rp1-sipspa.*version*.pkg	
			asr1000rp1-packages-adventservicesk9.*version*.conf	
			packages.conf	

1. The Cisco ASR 1000 Series RP1 ADVANCED IP SERVICES W/O CRYPTO consolidated package is only available with Cisco IOS XE Release 2.2.1 through Cisco IOS XE Release 2.3.*x*. This consolidated package is not available with any other Cisco IOS XE Releases.
2. The Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES W/O CRYPTO consolidated package is only available beginning with Cisco IOS XE Release 2.2.1 and later releases. This consolidated package is not available with Cisco IOS XE Release 2.1.2 and earlier releases.

Table 8 RP1 Memory Recommendations for the Cisco ASR 1000 Series Routers Optional Sub-package Image

Platforms	Image Name	Software Image	Flash Memory
Cisco ASR 1002 Router **Cisco ASR 1004 Router** **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP1 WebEx Node[1]	asr1000rp1-sipspawmak9.*version*.XND.pkg	100MB

1. The Cisco ASR 1000 Series RP1 WebEx Node (asr1000rp1-sipspawmak9.version.pkg) optional software sub-package 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 sub-package is not supported with earlier Cisco IOS XE releases or with any of the non-CRYPTO consolidated packages.

Note The RP2 images are available beginning with Cisco IOS XE Release 2.3.0.

Table 9 RP2 Memory Recommendations for the Cisco ASR 1000 Series Routers Consolidated Package Images

Platforms	Image Name	Software Image	Individual Sub-Package Contents	DRAM Memory
Cisco ASR 1004 Router **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP2 IP BASE W/O CRYPTO	asr1000rp2-ipbase.*version*.bin	asr1000rp2-rpbase.*version*.pkg	8GB-16GB(for Cisco ASR 1004 and Cisco ASR 1006 routers)
			asr1000rp2-rpcontrol.*version*.pkg	
			asr1000rp2-rpaccess.*version*.pkg	
			asr1000rp2-rpios-ipbase.*version*.pkg	
			asr1000rp2-espbase.*version.pkg*	
			asr1000rp2-sipbase.*version*.pkg	
			asr1000rp2-sipspa.*version*.pkg	
			asr1000rp2-packages-ipbase.*version*. conf	
			packages.conf	
Cisco ASR 1004 Router **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP2 IP BASE	asr1000rp2-ipbasek9.*version*.bin	asr1000rp2-rpbase.*version*.pkg	8GB-16GB(for Cisco ASR 1004 and Cisco ASR 1006 routers)
			asr1000rp2-rpcontrol.*version*.pkg	
			asr1000rp2-rpaccess.*version*.pkg	
			asr1000rp2-rpios-ipbasek9.*version*. pkg	
			asr1000rp2-espbase.*version*.pkg	
			asr1000rp2-sipbase.*version*.pkg	
			asr1000rp2-sipspa.*version*.pkg	
			asr1000rp2-packages-ipbasek9.*version*. conf	
			packages.conf	
Cisco ASR 1004 Router **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP2 ADVANCED IP SERVICES W/O CRYPTO[1]	asr1000rp2-advipservices.*version*. bin	asr1000rp2-rpbase.*version*.pkg	8GB-16GB(for Cisco ASR 1004 and Cisco ASR 1006 routers)
			asr1000rp2-rpcontrol.*version*.pkg	
			asr1000rp2-rpaccess.*version*.pkg	
			asr1000rp2-rpios-advipservices. *version*.pkg	
			asr1000rp2-espbase.*version*.pkg	
			asr1000rp2-sipbase.*version*.pkg	
			asr1000rp2-sipspa.*version*.pkg	
			asr1000rp2-packages-advipservices. *version*.conf	
			packages.conf	

Table 9 RP2 Memory Recommendations for the Cisco ASR 1000 Series Routers Consolidated Package Images

Platforms	Image Name	Software Image	Individual Sub-Package Contents	DRAM Memory
Cisco ASR 1004 Router **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP2 ADVANCED IP SERVICES	asr1000rp2-advipservicesk9.*version*.bin	asr1000rp2-rpbase.*version*.pkg	8GB-16GB(for Cisco ASR 1004 and Cisco ASR 1006 routers)
			asr1000rp2-rpcontrol.*version*.pkg	
			asr1000rp2-rpaccess.*version*.pkg	
			asr1000rp2-rpios-advipservicesk9.*version*.pkg	
			asr1000rp2-espbase.*version*.pkg	
			asr1000rp2-sipbase.*version*.pkg	
			asr1000rp2-sipspa.*version*.pkg	
			asr1000rp2-packages-advipservicesk9.*version*.conf	
			packages.conf	
Cisco ASR 1004 Router **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP2 ADVANCED ENTERPRISE SERVICES W/O CRYPTO	asr1000rp2-adventservices.*version*.bin	asr1000rp2-rpbase.*version*.pkg	8GB-16GB(for Cisco ASR 1004 and Cisco ASR 1006 routers)
			asr1000rp2-rpcontrol.*version*.pkg	
			asr1000rp2-rpaccess.*version*.pkg	
			asr1000rp2-rpios-adventservices.*version*.pkg	
			asr1000rp2-espbase.*version*.pkg	
			asr1000rp2-sipbase.*version*.pkg	
			asr1000rp2-sipspa.*version*.pkg	
			asr1000rp2-packages-adventservices.*version*.conf	
			packages.conf	
Cisco ASR 1004 Router **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP2 ADVANCED ENTERPRISE SERVICES	asr1000rp2-adventservicesk9.*version*.bin	asr1000rp2-rpbase.*version*.pkg	8GB-16GB(for Cisco ASR 1004 and Cisco ASR 1006 routers)
			asr1000rp2-rpcontrol.*version*.pkg	
			asr1000rp2-rpaccess.*version*.pkg	
			asr1000rp2-rpios-adventservicesk9.*version*.pkg	
			asr1000rp2-espbase.*version*.pkg	
			asr1000rp2-sipbase.*version*.pkg	
			asr1000rp2-sipspa.*version*.pkg	
			asr1000rp2-packages-adventservicesk9.*version*.conf	
			packages.conf	

1. The Cisco ASR 1000 Series RP2 ADVANCED IP SERVICES W/O CRYPTO consolidated package is only available with Cisco IOS XE Release 2.3.0 through the Cisco IOS XE Release 2.3.*x*. This consolidated package is not available with any other Cisco IOS XE Releases.

Table 10 RP2 Memory Recommendations for the Cisco ASR 1000 Series Routers Optional Sub-package Image

Platforms	Image Name	Software Image	Flash Memory
Cisco ASR 1004 Router **Cisco ASR 1006 Router**	Cisco ASR 1000 Series RP2 WebEx Node[1]	asr1000rp2-sipspawmak9.*version*.XND.pkg	100MB

1. The Cisco ASR 1000 Series RP2 WebEx Node (asr1000rp1-sipspawmak9.version.pkg) optional software sub-package 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 RP2 IP BASE, Cisco ASR 1000 Series RP2 ADVANCED IP SERVICES, or Cisco ASR 1000 Series RP2 ADVANCED ENTERPRISE SERVICES consolidated package. This sub-package is not supported with earlier Cisco IOS XE releases or with any of the non-CRYPTO consolidated packages.

Hardware Supported

Cisco IOS XE Release 2 supports the following Cisco ASR 1000 Series Routers:

- Cisco ASR 1002 Router
- Cisco ASR 1002-F Router
- Cisco ASR 1004 Router
- Cisco ASR 1006 Router

For descriptions of the new hardware features, see the "New and Changed Information" section on page 33.

ROMmon Version Requirements

This section describes the recommended and minimum ROMmon version requirements for Cisco IOS XE Release 2.

- The recommended ROMmon versions supported by the ROMmon upgradeable components for each Cisco IOS XE release are listed in the "Recommended ROMmon Versions for Cisco IOS XE Releases" subsection that follows.
- The minimum ROMmon versions required to support each specific ROMmon upgradeable component are listed in Table 11.

Recommended ROMmon Versions for Cisco IOS XE Releases

The recommended ROMmon version for Cisco IOS XE Release 2.6.0 and its rebuilds is Version 12.2(33r)XND1 for all ROMmon upgradeable components

The recommended ROMmon version for Cisco IOS XE Release 2.5.0 and its rebuilds is Version 12.2(33r)XND1 for all ROMmon upgradeable components

The recommended ROMmon version for Cisco IOS XE Release 2.4.0 and its rebuilds is Version 12.2(33r)XND1 for all ROMmon upgradeable components.

Note For customers requiring a FIPS 140-2 compliant environment, ROMmon Version 12.2(33r)XND is a required update.

The recommended ROMmon version to support the RP2 for Cisco IOS XE Release 2.3.2 is Version 12.2(33r)XNC0. The recommended ROMmon version to support the ASR1002, RP1, ESP5, ESP10, ESP10-N, ESP20, and SIP10 for Cisco IOS XE Release 2.3.2 is Version 12.2(33r)XNB.

The recommended ROMmon version to support the RP2 for Cisco IOS XE Release 2.3.1 is Version 12.2(33r)XNC0. The recommended ROMmon version to support the ASR1002, RP1, ESP5, ESP10, ESP10-N, ESP20, and SIP10 for Cisco IOS XE Release 2.3.1 is Version 12.2(33r)XNB.

The recommended ROMmon version to support the RP2 for Cisco IOS XE Release 2.3.0 is Version 12.2(33r)XNC0. The recommended ROMmon version to support the ASR1002, RP1, ESP5, ESP10, ESP10-N, ESP20, and SIP10 for Cisco IOS XE Release 2.3.0 is Version 12.2(33r)XNB.

The recommended ROMmon version for Cisco IOS XE Release 2.2.3 is Version 12.2(33r)XNB for all ROMmon upgradeable components.

The recommended ROMmon version for Cisco IOS XE Release 2.2.2 is Version 12.2(33r)XNB for all ROMmon upgradeable components.

The recommended ROMmon version for Cisco IOS XE Release 2.2.1 is Version 12.2(33r)XNB for all ROMmon upgradeable components.

The recommended ROMmon version supported for Cisco IOS XE Release 2.1.2 is Version 12.2(33r)XN2 for all ROMmon upgradeable components.

The recommended ROMmon version supported for Cisco IOS XE Release 2.1.1 is Version 12.2(33r)XN2 for all ROMmon upgradeable components.

The recommended ROMmon version supported for Cisco IOS XE Release 2.1.0 is Version 12.2(33r)XN2 for all ROMmon upgradeable components.

Note The minimum ROMmon version supported for Cisco IOS Release 2.1.x and later releases is Version 12.2(33r)XN2. Version 12.2(33r)XN2 is required to support the Cisco ASR 1002 Router. If support is not required for the Cisco ASR 1002 Router, the minimum ROMmon version required is Version 12.2(33r)XN1.

Table 11 Minimum ROMmon Version Required to Support ROMmon Upgradeable Components

ROMmon Upgradeable Component	12.2(33r)XN2	12.2(33r)XNB	12.2(33r)XNC0	12.2(33r)XND1
ASR1002[1]	X			X
ASR1002-F[2]	X			X
RP1	X			X
RP2			X	X[3]
ESP5	X			
ESP10	X			
ESP10-N		X		
ESP20		X		
SIP10	X			

1. ROMmon upgradeable components on the ASR1002: integrated RP1, field-replaceable ESP, and integrated SIP10.
2. ROMmon upgradeable components on the ASR1002-F: integrated RP1, ESP, and SIP10.

3. In 12.2(33r)XND1, when ROMmon is upgraded on RP2, **show platform** displays 12.2(33r)XND.

Determining the Software 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:

```
Router# show version
Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-IPBASE-M), Version 12.2(33)XNF2,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 07-Jul-10 01:35 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2010 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 06:05:49 UTC Wed Jul 7 2010
System image file is "tftp:/auto/tftp-smoke2/mcpdt-6ru-15/vmlinux"
Last reload reason: PowerOn


cisco ASR1006 (RP2) processor with 4407369K/6147K bytes of memory.
5 Gigabit Ethernet interfaces
2 Packet over SONET interfaces
2 Channelized T3 ports
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1925119K bytes of eUSB flash at bootflash:.
78085207K bytes of SATA hard disk at harddisk:.

Configuration register is 0x2
```

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

Note The checksums in the **show version installed** output that follows are for example purposes only; the checksum values that appear in your output may vary.

```
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: 00b8d95bd6aa71795d9817492dfe2723a4cf7ca2

Package: rpbase, version: 02.06.02.122-33.XNF2, status: active
  File: consolidated:asr1000rp2-rpbase.02.06.02.122-33.XNF2.pkg, on: RP0
  Built: 2010-07-07_03.10, by: mcpre
  File SHA1 checksum: a6b9bea258d081075e65e8fe1867d5d680f85703

Package: rpcontrol, version: 02.06.02.122-33.XNF2, status: active
  File: consolidated:asr1000rp2-rpcontrol.02.06.02.122-33.XNF2.pkg, on: RP0/0
  Built: 2010-07-07_03.10, by: mcpre
  File SHA1 checksum: 54ac3da1473dd1e37796b1f5afa83b5c4a96f537

Package: rpios-ipbase, version: 02.06.02.122-33.XNF2, status: active
  File: consolidated:asr1000rp2-rpios-ipbase.02.06.02.122-33.XNF2.pkg, on: RP0/0
  Built: 2010-07-07_03.12, by: mcpre
  File SHA1 checksum: ffcd38ab5a39537121c83c23067459a9c1b485cb

Package: rpaccess, version: 02.06.02.122-33.XNF2, status: active
  File: consolidated:asr1000rp2-rpaccess.02.06.02.122-33.XNF2.pkg, on: RP0/0
  Built: 2010-07-07_03.10, by: mcpre
  File SHA1 checksum: ffccabb82f70fd6a21ad5a3128585104d6508965

Package: rpcontrol, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-rpcontrol.02.06.02.122-33.XNF2.pkg, on: RP0/1
  Built: 2010-07-07_03.10, by: mcpre
  File SHA1 checksum: 54ac3da1473dd1e37796b1f5afa83b5c4a96f537

Package: rpios-ipbase, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-rpios-ipbase.02.06.02.122-33.XNF2.pkg, on: RP0/1
  Built: 2010-07-07_03.12, by: mcpre
  File SHA1 checksum: ffcd38ab5a39537121c83c23067459a9c1b485cb

Package: rpaccess, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-rpaccess.02.06.02.122-33.XNF2.pkg, on: RP0/1
  Built: 2010-07-07_03.10, by: mcpre
  File SHA1 checksum: ffccabb82f70fd6a21ad5a3128585104d6508965

Package: rpbase, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-rpbase.02.06.02.122-33.XNF2.pkg, on: RP1
  Built: 2010-07-07_03.10, by: mcpre
  File SHA1 checksum: a6b9bea258d081075e65e8fe1867d5d680f85703

Package: rpcontrol, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-rpcontrol.02.06.02.122-33.XNF2.pkg, on: RP1/0
  Built: 2010-07-07_03.10, by: mcpre
  File SHA1 checksum: 54ac3da1473dd1e37796b1f5afa83b5c4a96f537

Package: rpios-ipbase, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-rpios-ipbase.02.06.02.122-33.XNF2.pkg, on: RP1/0
  Built: 2010-07-07_03.12, by: mcpre
  File SHA1 checksum: ffcd38ab5a39537121c83c23067459a9c1b485cb

Package: rpaccess, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-rpaccess.02.06.02.122-33.XNF2.pkg, on: RP1/0
  Built: 2010-07-07_03.10, by: mcpre
  File SHA1 checksum: ffccabb82f70fd6a21ad5a3128585104d6508965

Package: rpcontrol, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-rpcontrol.02.06.02.122-33.XNF2.pkg, on: RP1/1
  Built: 2010-07-07_03.10, by: mcpre
  File SHA1 checksum: 54ac3da1473dd1e37796b1f5afa83b5c4a96f537

Package: rpios-ipbase, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-rpios-ipbase.02.06.02.122-33.XNF2.pkg, on: RP1/1
```

```
  Built: 2010-07-07_03.12, by: mcpre
  File SHA1 checksum: ffcd38ab5a39537121c83c23067459a9c1b485cb

Package: rpaccess, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-rpaccess.02.06.02.122-33.XNF2.pkg, on: RP1/1
  Built: 2010-07-07_03.10, by: mcpre
  File SHA1 checksum: ffccabb82f70fd6a21ad5a3128585104d6508965

Package: espbase, version: 02.06.02.122-33.XNF2, status: active
  File: consolidated:asr1000rp2-espbase.02.06.02.122-33.XNF2.pkg, on: ESP0
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: f27b18ddc451406d23fd849e3a1b405f72531028

Package: espbase, version: 02.06.02.122-33.XNF2, status: active
  File: consolidated:asr1000rp2-espbase.02.06.02.122-33.XNF2.pkg, on: ESP1
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: f27b18ddc451406d23fd849e3a1b405f72531028

Package: sipbase, version: 02.06.02.122-33.XNF2, status: active
  File: consolidated:asr1000rp2-sipbase.02.06.02.122-33.XNF2.pkg, on: SIP0
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: 57de38b3a28e2bfe613eb1c14d14758eeced0bee

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP0/0
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: active
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP0/1
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: active
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP0/2
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: active
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP0/3
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipbase, version: 02.06.02.122-33.XNF2, status: active
  File: consolidated:asr1000rp2-sipbase.02.06.02.122-33.XNF2.pkg, on: SIP1
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: 57de38b3a28e2bfe613eb1c14d14758eeced0bee

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP1/0
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP1/1
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP1/2
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
```

```
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP1/3
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipbase, version: 02.06.02.122-33.XNF2, status: active
  File: consolidated:asr1000rp2-sipbase.02.06.02.122-33.XNF2.pkg, on: SIP2
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: 57de38b3a28e2bfe613eb1c14d14758eeced0bee

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP2/0
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP2/1
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP2/2
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP2/3
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipbase, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipbase.02.06.02.122-33.XNF2.pkg, on: SIP3
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: 57de38b3a28e2bfe613eb1c14d14758eeced0bee

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP3/0
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP3/1
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP3/2
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP3/3
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipbase, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipbase.02.06.02.122-33.XNF2.pkg, on: SIP4
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: 57de38b3a28e2bfe613eb1c14d14758eeced0bee

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP4/0
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e
```

```
Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP4/1
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP4/2
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP4/3
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipbase, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipbase.02.06.02.122-33.XNF2.pkg, on: SIP5
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: 57de38b3a28e2bfe613eb1c14d14758eeced0bee

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP5/0
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP5/1
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP5/2
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e

Package: sipspa, version: 02.06.02.122-33.XNF2, status: n/a
  File: consolidated:asr1000rp2-sipspa.02.06.02.122-33.XNF2.pkg, on: SIP5/3
  Built: 2010-07-07_02.56, by: mcpre
  File SHA1 checksum: fca726414781540f44dc166859a786bd1dc6279e
```

Cisco IOS XE to Cisco IOS Version Number Mapping

Each version of Cisco IOS XE has an associated Cisco IOS version. Table 12 lists these mappings for all released versions of Cisco IOS XE.

Table 12 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOS Version
02.01.00	12.2(33)XNA
02.01.01	12.2(33)XNA1
02.01.02	12.2(33)XNA2
02.02.01	12.2(33)XNB1
02.02.02	12.2(33)XNB2
02.02.03	12.2(33)XNB3
02.03.00 (Deferred Version)	12.2(33)XNC (Deferred Version)
02.03.00t	12.2(33)XNC0t
02.03.01 (Deferred Version)	12.2(33)XNC1 (Deferred Version)
02.03.01t	12.2(33)XNC1t
02.03.02	12.2(33)XNC2
02.04.00	12.2(33)XND
02.04.01	12.2(33)XND1
02.04.02	12.2(33)XND2
02.04.02t	12.2(33)XND2t
02.04.03	12.2(33)XND3
02.04.04	12.2(33)XND4
02.05.00	12.2(33)XNE
02.05.01	12.2(33)XNE1
02.05.02	12.2(33)XNE2
02.06.00	12.2(33)XNF
02.06.01	12.2(33)XNF1
02.06.02	12.2(33)XNF2

Note The Cisco IOS XE 2.3.0 and Cisco IOS XE 2.3.1 images are no longer downloadable from Cisco.com. Replacement images (Cisco IOS XE 2.3.0t and Cisco IOS XE 2.3.1t) with exactly the same content and bug fixes are available on Cisco.com. If the Cisco IOS XE 2.3.0 and Cisco IOS XE 2.3.1 images are not causing any issues, no action is necessary. Old image MD5 sums will still be available for verification on the download page. For more details, see CSCsz80074.

Upgrading to a New Software Release

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

For information about upgrading to a new software release, see the following document:

Cisco ASR 1000 Series Aggregation Services Router Software Configuration Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/asrswcfg.html

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 2 and contains the following sections:

New Hardware Features in Cisco IOS XE Release 2.6.2

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.6.2.

New Software Features in Cisco IOS XE Release 2.6.2

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.6.2.

New Hardware Features in Cisco IOS XE Release 2.6.1

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.6.1.

New Software Features in Cisco IOS XE Release 2.6.1

This section lists new and changed features in Cisco IOS XE Release 2.6.1. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS XE:

Active Probe Source Address

This feature allows for user configurable source address for Optimized Edge Routing (OER) Active Probes.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/pfr/configuration/guide/pfr-advanced.html

CUBE(SP Edition) - Billing:Packet Cable Billing support for Adjacency Information

For information about these Cisco Unified Border Element (SP Edition) features, see the following documents:

Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/2_xe/sbcu_2_xe_book.html

Cisco Unified Border Element (SP Edition) Command Reference: Unified Model

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

OER - Application Aware Routing with Static Application Mapping

This feature allows for optimize application traffic using PBR (Policy Based Routing).

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/pfr/configuration/guide/pfr-stat-app-map.html

OER Border Router Only Functionality

Optimized Edge Routing (OER) Border Router master controller software has been modified to handle the limited functionality.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/pfr/configuration/guide/pfr-br-only_xe.html

OER - Inbound Optimization through BGP

This feature allows for Optimized Edge Routing (OER) monitors and optimizes inbound (to enterprise) traffic using BGP advertisements to BGP external peers.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/pfr/configuration/guide/pfr-bgp-inbound.html

OER Port and Protocol Based Prefix Learning

OER Port and Protocol Based Prefix Learning allows one to configure a master controller to learn prefixes based on the protocol type and TCP or UDP port number.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/pfr/configuration/guide/pfr-understand.html

OER Support for Cost-Based Optimization and Traceroute Reporting

This enhancement provides outbound traffic optimization based on financial link cost (i.e., fixed cost versus tier based cost). This release also adds support for traceroute reporting.

For more information, see the following documents:

http://www.cisco.com/en/US/docs/ios/pfr/configuration/guide/pfr-trace.html

http://www.cisco.com/en/US/docs/ios/pfr/configuration/guide/pfr-cost.html

OER Support for Policy-Rules Configuration and Port-Based Prefix Learning

OER support for policy-rule configuration and port-based prefix learning.

For more information, see the following documents:

http://www.cisco.com/en/US/docs/ios/pfr/configuration/guide/pfr-advanced.html

http://www.cisco.com/en/US/docs/ios/pfr/configuration/guide/pfr-understand.html

OER VPN IPSec with GRE Tunnel Optimization

VPN IPSec/GRE Tunnel Optimization introduces the capability to configure IPSec with GRE tunnel interfaces as OER managed exit links. Only network based IPSec VPNs are supported.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/pfr/configuration/guide/pfr-gre-exit.html

OER - Voice Traffic Optimization

This feature allows for Optimize Route Control for Voice traffic on the network.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/pfr/configuration/guide/pfr-voice-traffic.html

PfR EIGRP mGRE DMVPN Hub-and-Spoke Support

This gives PfR the ability to inject routes into the EIGRP routing table in order to control prefixes and applications over EIGRP routes. Also adds support for mGRE DMVPN deployments. Currently only supports Hub- and-Spoke, not Spoke-to-Spoke

For more information, see the following document

http://www.cisco.com/en/US/docs/ios/pfr/configuration/guide/pfr-eigrp-mgre.html

PfR - Protocol Independent Route Optimization (PIRO)

This feature removes the requirement of having BGP or static parent routes and allows PfR to operate with any routing protocol.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/pfr/configuration/guide/pfr-piro.html

New Hardware Features in Cisco IOS XE Release 2.6.0

The following hardware features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.6.0:

1-Port Channelized OC-12/STM-4 SPA (SPA-1XCHOC12/DS0)

The 1-Port Channelized OC-12/STM-4 SPA is a double-height serial SPA that can be installed into two, vertically-aligned SIP subslots. The channelized OC-12 SPA with small form-factor pluggable (SFP) optical transceiver modules provides SONET network connectivity with a per-port bandwidth of 622.08 Mbps, and supports channelization from OC-12 down to DS0 line rates.

For information about the 1-Port Channelized OC-12/STM-4 SPA and other SPAs supported on the Cisco ASR 1000 Series Routers, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide at:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/ASR1000/asr_sip_spa_hw.html

Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide at:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ASR1000/ASRspasw.html

New Software Features in Cisco IOS XE Release 2.6.0

This section lists new and changed features in Cisco IOS XE Release 2.6.0. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS XE:

AAA: Supress System Accounting On Switchover

Suppressing System Accounting Records over Switchover allows to suppress the system accounting-on and accounting-off messages during switchover.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_accountg_ps10591_TSD_Products_Configuration_Guide_Chapter.html

ASRNAT - Overload Scaling Improvement - Support 800 Overloaded Pools

Network Address Translation (NAT) now supports 800 overloaded pools on Cisco ASR 1000 series Routers with a 20-Gbps Embedded Services Processor (ESP).

BGP Event Based VPN Import

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_event_vpn_import_xe.html

BGP RT Changes Without PE-CE Neighbor Impact

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-event-vpn-import.html

BGP Support for the L2VPN Address Family

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_overview.html

Broadband IPv6 Support at LNS

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-adsl_dial_xe.html

Call Home

The Call Home feature provides e-mail-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications. Common uses of this feature may include direct paging of a network support engineer, e-mail notification to a Network Operations Center, XML delivery to a support website, and utilization of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

For more information, see the feature documentation in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide at:

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/callhome_asr1k.html

CLNS Support for GRE Tunneling of IPv4 and IPv6

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/isoclns/configuration/guide/configure_iso_clns.html

Control Plane DSCP Support for RSVP

This feature allows for RSVP control message precedence and DSCP support.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/dscp_spt_for_rsvp_xe.html

DHCP VRF Exclude Support

Today there is no way for the user/administrator to exclude IP address range in different VRF address spaces. The intention of this work is to extend the present command line interface support creation of IP address exclusion list in different address spaces.For more information, see the following document:

EIGRP Prefix Limit Support

The EIGRP Prefix Limit Support the feature allows for EIGRP Provider and Customer Edge Prefix Limit Support.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_eigrp/configuration/guide/ire_pref_limit_xe.html

Enabling OSPFv2 on an Interface Basis

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_ospf/configuration/guide/iro_mode_ospfv2_xe.html

IGMP MIB Support Enhancements for SNMP

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to neighboring multicast routers. The IGMP MIB describes objects that enable users to remotely monitor and configure IGMP using Simple Network Management Protocol (SNMP). It also allows users to remotely subscribe and unsubscribe from multicast groups. The IGMP MIB Support Enhancements for SNMP feature adds full support of RFC 2933 (Internet Group Management Protocol MIB) in Cisco IOS software.

There are no new or modified Cisco IOS commands associated with this feature.

For detailed information about the IGMP MIB, see the IGMP-STD-MIB.my file available from the Cisco MIB Locator at http://www.cisco.com/go/mibs.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipmulti/configuration/guide/imc_igmp_static_rng_xe.html

IGMP Static Group Range Support

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_igmp/configuration/xe-3s/IGMP_Static_Group_Range_Support.html

IGMPv3 Host Stack

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_customize_igmp.html

IP-RIP Delay Start

The IP-RIP Delay Start feature is used when a Cisco ASR Router is configured to establish a RIPv2 neighbor relationship using MD5 authentication with a non-Cisco device over a Frame Relay network.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_rip/configuration/guide/irr_cfg_rip_xe.html

IPv6 - Full Selective Packet Discard (SPD) Support

IPv6 Full Selective Packet Discard (SPD) feature restores parity between SPD function for IPv4 and IPv6.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-spd_xe.html

IPv6 - Per Interface Neighbor Discovery Cache Limit

IPv6 - Per interface Neighbor Discovery Cache Limit feature allows for a number of entries in the ND cache is limited on an interface basis. Once the limit is reached, no new entries are allowed.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-addrg_bsc_con_xe.html

IPv6 ISIS Local RIB

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-is-is_xe.html

IPv6 Multicast: Bandwidth-Based Call Admission Control (CAC)

The Bandwidth Based CAC for IPv6 Multicast feature implements a method to monitor bandwidth per interface and multicast group avoiding oversubscription due to multicast services.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-is-is_xe.html

IPv6 PIM Passive

IPv6 PIM Passive feature enable PIM passive mode on interface. PIM passive interface doesnt send and receive PIM control messages but it can act as RPF interface for multicast route entries and accept/forward multicast data packet.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html

IPv6 Routing: IS-IS Multitopology Support for IPv6

Support for routing IPv6 Prefixes in IS-IS is using a multi-topology solution.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-is-is_xe.html

IPv6: Multicast Address Group Range Support

IPv6 Multicast Address Group Range feature allows for disables all operations for groups denied by <acl>. Drop/ignore group in all control packets - PIM, MLD.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html

IS-IS Fast-Flooding of LSPs Using the fast-flood Command

The IS-IS Fast-Flooding of LSPs Using the fast-flood Command feature improves Intermediate System-to-Intermediate System (IS-IS) convergence time when new link-state packets (LSPs) are generated in the network and SPF is triggered by the new LSPs.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/xe-3s/Reducing_Link_Failure_and_Topology_Change_Notification_Times_in_IS-IS_Networks.html

IS-IS Limit on Number of Redistributed Routes

The IS-IS Limit on Number of Redistributed Routes feature provides for a user-defined maximum number of prefixes that are allowed to be redistributed into IS-IS from other protocols or other IS-IS processes. Such a limit can help prevent the router from being flooded by too many redistributed routes.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_isis/configuration/guide/irs_fscpc_xe.html

IS-IS Support for Route Tags

The IS-IS Support for Route Tags feature provides the capability to tag IS-IS route prefixes and use those tags in a route map to control IS-IS route redistribution or route leaking.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_isis/configuration/guide/irs_fscpc_xe.html

Lawful Intercept (LI)

In Cisco IOS XE Release 2.6, pre-provisioning of circuit-ID based tapping of a PPP session is introduced. If the tap is provisioned before a user session is active, then the tap is effective whenever the user session becomes active. Also, corresponding RADIUS authentication and accounting packets are tapped. It is assumed in this instance that the user session is uniquely identified by a circuit ID tag.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/sec_user_services/configuration/guide/sec_lawful_intercept_xe.html

Layer 2 Tunnel Protocol Version 3

The Layer 2 Tunnel Protocol Version 3 (L2TPv3) feature expands Cisco support of Layer 2 Tunnel Protocol (L2TP). L2TPv3 is an Internet Engineering Task Force (IETF) Layer Two Tunneling Protocol Extensions (l2tpext) working group draft that provides several enhancements to L2TP for the capability to tunnel any Layer 2 payload over L2TP. Specifically, L2TPv3 defines the L2TP protocol for tunneling Layer 2 payloads over an IP core network using Layer 2 Virtual Private Networks (VPNs).

In addition Cisco IOS XE Release 2.6.0 introduces support for the following Layer 2 Tunnel Protocol Version 3 (L2TPv3) features:

- Ethernet over L2TPv3
- IfTable MIB for attachment circuit
- L2TPv3 - Layer-2 Tunneling Protocol Version 3
- L2TPv3 Basic Features
- L2TPv3 Control Message Hashing
- L2TPv3 Control Message Rate Limiting
- L2TPv3 Digest Secret Graceful Switchover
- L2TPv3: Custom Ethertype for Dot1Q and QinQ encapsulations
- L2TPv3: Remote Ethernet Port Shutdown
- Layer 2 VPN (L2 VPN): Syslog, SNMP Trap, and show Command Enhancements for AToM and L2TPv3
- Protocol Demultiplexing for L2TPv3

MLD Group Limits

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html

MPLS MTU command for GRE Tunnels

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/xe-3s/mp-any-transport-xe.html

MPLS TE--Tunnel-Based Admission Control (TBAC)

Tunnel Based Admission Control Phase.1 addresses the need to aggregate RSVP flows into a static multi-hop MPLS-TE tunnel. It is based on RFC 4804.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/xe-3s/MPLS_TE_-_Tunnel-Based_Admission_Control.html

Multicast Address Group Range Support

The Multicast Address Group Range Support feature enhances multicast access control by introducing the capability to define a global range of multicast groups and channels to be permitted or denied using the ip multicast group-range command.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/2/release/notes/rnasr21.html

Multicast MIB VRF Support

The Multicast VRF MIB Support feature is an enhancement to help manage Cisco devices in a multicast VPN environment using SNMP.

This feature enhances the Cisco suite of supported multicast MIBs by making the following multicast MIBs MVRF aware:

CISCO-IPMROUTE-MIB

CISCO-PIM-MIB

IGMP-STD-MIB

IPMROUTE-STD-MIB

MSDP-MIB

PIM-MIB

Multicast VRF (MVRF) awareness enables the MIB objects associated with these Multicast MIBs to be queried and set for the individual MVRFs configured. In addition, MVRF awareness provides the capability to detect conditions for a trap inside of a MVRF and lookup the correct information for that MVRF; the traps would then be sent to the SNMP manager that is configured for that MVRF.

For detailed information about these MIBs, and to locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at http://www.cisco.com/go/mibs.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/2/release/notes/rnasr21.html

Multiprotocol BGP (MP-BGP) Support for CLNS

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_sup_clns_xe.html

Netflow Data Export to a collector in a VRF

This feature enables export of netflow data to a destination whose route is in a virutal routing table other than the global table.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/netflow/command/reference/nf_01.html#wp1049093

OSPF Link-State Advertisement Throttling

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_ospf/configuration/guide/iro_lsa_throt_xe.html

OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements

This feature provides OSPF mechanism to exclude IP prefixes of connected networks from link state advertisements (LSAs), thereby reducing OSPF convergence time.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_ospf/configuration/guide/iro_ex_lsa_xe.html

OSPF Sham-Link MIB Support

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_ospf/configuration/guide/iro_sham_mib_xe.html

OSPF SNMP ifIndex Value for Interface ID

A configuration command will be added to the router ospf configuration for both OSPFv2 and OSPFv3 which, when enabled, will cause OSPF to use the SNMP MIB-II ifIndex number to identify interfaces.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_ospf/configuration/guide/iro_snmp_ifindex_xe.html

OSPF Limit on Number of Redistributed Routes

OSPF support for setting a maximum number of prefixes to be redistributed/imported from other protocols (SSO Capable).

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_ospf/configuration/guide/iro_lim_routes_xe.html

PIM Triggered Joins

The PIM Triggered Joins feature is a multicast HA enhancement that improves the reconvergence of mroutes after an RP switchover. In the event of an RP switchover, this feature utilizes the PIM-SM GenID value as a mechanism to trigger adjacent PIM neighbors on an interface to send PIM join messages for all (*, G) and (S, G) mroutes that use that interface as an RPF interface, immediately reestablishing those states on the newly active RP.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipmulti/configuration/guide/imc_high_availability_xe.html

Quality of Service: Policies Aggregation

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/qos_policies_agg_xe.html

RSVP Aggregation

Flow aggregation is a mechanism wherein RSVP state can be reduced in a router by aggregating many smaller reservations into a single larger reservation.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/qos_rsvp_agg_xe.html

RSVP Application ID Support

This feature enhances RSVP to integrate with the IGP routewatch functionality, which will allow it to respond to routing changes with sub-second response time.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/rsvp_app_id_support_xe.html

RSVP Fast Local Repair (RSVP FLR)

This feature enhances RSVP to integrate with the IGP routewatch functionality, which will allow it to respond to routing changes with sub-second response time.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/rsvp_fast_local_rpr_xe.html

RSVP Interface-based Receiver Proxy

This feature allows for RSVP Receiver Proxy configuration based on outbound interface.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/rsvp_receiver_proxy_xe.html

RSVP Scalability Enhancements

RSVP feature enhancements will improve the ASR 1000 Router Series performance and scalability.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/rsvp_scalability_xe.html

RSVP Support for IP Sessions

The RSVP Support for IP Sessions feature allows Resource Reservation Protocol (RSVP) and Intelligent Services Gateway (ISG) to coexist in a structured framework in which edge access devices can deliver flexible and scalable services that include voice on demand (VoD) call admission control (CAC) to subscribers.

SNMP Traps for PPPoE Session Limits

The SNMP traps for PPPoE session limits feature implements SNMP MIB support for PPPoE session limits which are configured using the following **bba-group** commands:

Session Limit/Throttle **bba-group** command

per-mac limit	**sessions per-mac limit** <n>
	sessions per-mac iwf limit <n>
per-vlan limit	**sessions per-vlan limit** <n>
per-vc limit	**sessions per-vc limit** <n>

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/bbdsl/configuration/xe-3s/bba-mon-pppoe-snmp-xe.html

Support for Software Media Termination Point (MTP) on the Cisco Unified Border Element (Enterprise)

A software Media Termination Point (MTP) bridges the media streams between two connections allowing Cisco Unified Communications Manager to relay calls that are routed through SIP or H.323 endpoints via Skinny Call Control Protocol (SCCP) commands. This feature extends the software MTP support to the Cisco Unified Border Element (Enterprise).

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_proto/configuration/xe-3s/support_for_software_media_termination_point.html

T.38 Fax Support on the Cisco Unified Border Element (Enterprise)

This feature allows for the use of T.38 fax relay on an IP network. T.38 is an ITU standard that defines how fax communications are packetized and transported over IP networks. This feature extends the T.38 fax signaling and T.38 fax over UDP packets support to the Cisco Unified Border Element (Enterprise).

There are no new or modified command introduced by this feature.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/config_library/xe-3s/cube-xe-3s-library.html

VRF Aware IPSec

The VRF-Aware IPsec feature introduces IP Security (IPsec) tunnel mapping to Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Using the VRF-Aware IPsec feature, you can map IPsec tunnels to Virtual Routing and Forwarding (VRF) instances using a single public-facing address.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/sec_vrf_aware_ipsec_xe.html

VRRP MIB - RFC2787

The VRRP MIB RFC2787 this allows for RFC2787 support.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipapp/configuration/guide/ipapp_vrrp_xe.html

VRRP: Virtual Router Redundancy (VRRS)

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipapp/configuration/guide/ipapp_vrrs_xe.html

Zone Based Firewall: Default Zone

Enable firewall policy to be configured on a zone pair which consist of a zone and a default zone. Any interface without explicit zone membership belongs to default zone.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/sec_data_plane/configuration/guide/sec_zone_polcy_firew_xe.html

Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model

The following Cisco Unified Border Element (SP Edition) features were introduced in Cisco IOS XE Release 2.6.0:

- CUBE(SP Edition) CODEC Enhancements
- CUBE(SP Edition) Unsignaled Secure Media
- CUBE(SP Edition): DBE: Optional TMAN Bandwidth Parameter Policing
- CUBE(SP Edition): DBE: Return Local and Remote Descriptors in H.248 Reply
- CUBE(SP Edition): SIP:Contact Username Passthrough (non-IMS case)
- CUBE(SP Editon): SIP:Interoperability for SIP Authentication
- SBC End Point Switching
- SIP Non-SDP Body Filtering
- SIP: SIP SDP and Body Filtering
- Source Number Analysis

In addition Cisco IOS XE Release 2.6.0 introduces support for the following CUBE(SP Edition) IPv6 Support:

- SIP:DNS support for IPv6
- Media:IPv6-IPv6 (RTP)
- SIP:SIP Signaling IPv4 to IPv6 interworking
- SIP:SIP Signaling Over IPv6
- SIP:SIP Media IPv4 to IPv6 interworking

For information about these Cisco Unified Border Element (SP Edition) features, see the following documents:

Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/2_xe/sbcu_2_xe_book.html

Cisco Unified Border Element (SP Edition) Command Reference: Unified Model

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

New Hardware Features in Cisco IOS XE Release 2.5.2

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.5.2.

New Software Features in Cisco IOS XE Release 2.5.2

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.5.2.

New Hardware Features in Cisco IOS XE Release 2.5.1

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.5.1.

New Software Features in Cisco IOS XE Release 2.5.1

This section lists new and changed features in Cisco IOS XE Release 2.5.1. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS XE:

- VRF-Aware Local Area Mobility (LAM)

  VRF-Awareness in LAM provides the ability to distinguish two destinations with the same IP address.

  For more information, see the following document:

  http://preview.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_01.html#wp1020438

Cisco Unified Border Element (SP Edition)

The following Cisco Unified Border Element (SP Edition) features were introduced in Cisco IOS XE Release 2.5.1:

- CUBE(SP Editon): H.323:H.323 TCS Codecs Support

For information about these Cisco Unified Border Element (SP Edition) features, see the following documents:

Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/2_xe/sbcu_2_xe_book.html

Cisco Unified Border Element (SP Edition) Command Reference: Unified Model

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

New Hardware Features in Cisco IOS XE Release 2.5.0

The following hardware features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.5.0:

1-Port Clear Channel OC-12 ATM SPA (SPA-1XOC12-ATM-v2)

The 1-Port Clear Channel OC-12 ATM SPA is a single-height ATM SPA that can be installed into one SIP subslot. The OC-12 ATM SPA with small form-factor pluggable (SFP) optical transceiver modules provides SONET and SDH network connectivity with a per-port bandwidth of 622.08 Mbps.

For information about the SPAs supported on the Cisco ASR 1000 Series Routers, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide at the following location:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/ASR1000/asr_sip_spa_hw.html

Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide at the following location:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ASR1000/ASRspasw.html

New XFP/SFPs Supported with SPAs and the Built-In Gigabit Ethernet Interface

The following transceiver modules are newly supported on the Cisco ASR 1000 Series Routers for the following SPAs:

- Cisco10GBASE-SR XFP transceiver module for MMF, 850-nm wavelength, dual LC connector (XFP-10G-MM-SR)—Supported with the 1-Port 10-Gigabit Ethernet SPA (SPA-1X10GE-L-V2) only on the Cisco ASR-1002, Cisco ASR-1004, and Cisco ASR-1006 routers.
- Cisco1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength (GLC-BX-D)—Supported with the following hardware:
  - 2-Port Gigabit Ethernet SPA (SPA-2X1GE-V2)
  - 5-Port Gigabit Ethernet SPA (SPA-5X1GE-V2)
  - 10-Port Gigabit Ethernet SPA (SPA-10X1GE-V2)
  - Built-in Gigabit Ethernet interface on the Cisco ASR-1002 router
- Cisco 1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength (GLC-BX-U)—Supported with the following hardware:
  - 2-Port Gigabit Ethernet SPA (SPA-2X1GE-V2)
  - 5-Port Gigabit Ethernet SPA (SPA-5X1GE-V2)
  - 10-Port Gigabit Ethernet SPA (SPA-10X1GE-V2)
  - Built-in Gigabit Ethernet interface on the Cisco ASR-1002 router

For more information, see the following publications:

- For information on optics module compatibility with SPAs on the Cisco ASR 1000 series routers, see the "Modular Optics Compatibility" section of the "SIP and SPA Overview" chapter in the Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide at:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/ASR1000/ASRintro.html

- For more information about the built-in Gigabit Ethernet interface on the Cisco ASR-1002 routers and optics module compatibility, see the Cisco ASR 1000 Series Aggregation Services Router Hardware Installation Guide at:

  http://www.cisco.com/en/US/docs/routers/asr1000/install/guide/asr1routers/asr1higV8.html

- For more information about a specific supported transceiver module and its installation and maintenance, find the corresponding documentation for the supported module at the Cisco Transceiver Modules site at:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

New Software Features in Cisco IOS XE Release 2.5.0

This section lists new and changed features in Cisco IOS XE Release 2.5. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS XE Release 2.5:

2547oDMVPN - Enabling Traffic Segmentation within DMVPN

Cisco IOS XE Release 2.5 provides an enhancement that allows you to segment VPN traffic within a DMVPN tunnel.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/sec_DMVPN_xe.html

AAA - Improvements for Broadband IPv6

This feature is supported in Cisco IOS XE Release 2.5.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-adsl_dial_xe.html

ANCP - ATM Support

You can enable ANCP support on an ATM interface by using the **enable ancp** command. This is one of the optional steps for configuring PVC.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/atm/configuration/guide/atm_cfg_atm_xe.html

ATM F4 Ping

The F4 Operations, Administration, and Maintenance (OAM) Ping without Virtual Path (VP) Creation feature enables you to determine problems at the virtual path (VP) level using the ping command. Using

this feature, you can create and remove virtual circuit identifiers (VCIs) that correspond to the VP segment and the VP end, in the absence of VP configuration. After creating the VCIs you can use the ping atm command to isolate connection problems.

ATM Sub-interface Multipoint

ATM supports two types of interfaces: point-to-point and multipoint.

- Point-to-point subinterface—With point-to-point subinterfaces, each pair of routers has its own subnet. If you put the PVC on a point-to-point subinterface, the router assumes that there is only one point-to-point PVC configured on the subinterface. Therefore, any IP packets with a destination IP address in the same subnet are forwarded on this virtual circuit (VC). This is the simplest way to configure the mapping and is therefore the recommended method.
- - Multipoint networks—Multipoint networks have three or more routers in the same subnet. If you put the PVC in a point-to-multipoint subinterface or in the main interface (which is multipoint by default), you need to either configure a static mapping or enable inverse Address Resolution Protocol (ARP) for dynamic mapping.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/atm/configuration/guide/atm_cfg_atm_xe.html

ATM VC Ingress Policing

This feature module describes how to configure QoS hierarchical queueing policy maps on sessions and ATM VCs in ATM Digital Subscriber Line Access Multiplexer (A-DSLAM) applications.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/ppp_ses_que_atm_vc_xe.html

BGP Best External

The BGP Best External feature provides the capability of configuring the additional backup paths and advertises the best-external route which is the most preferred route among the routes received by a router from its eBGP peers. The best-external route can be used in case the primary PE fails or the primary PE link fails thereby reducing traffic loss and aiding in achieving faster PIC time.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_best_external_xe.html

BGP Multicast Inter-AS (IAS) VPN

The BGP Best External feature provides the capability of configuring the additional backup paths and advertises the best-external route which is the most preferred route among the routes received by a router from its eBGP peers. The best-external route can be used in case the primary PE fails or the primary PE link fails thereby reducing traffic loss and aiding in achieving faster PIC time.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_best_external_xe.html

BGP PIC Edge for IP/MPLS

The BGP PIC feature provides the ability to converge BGP routes within sub-seconds instead of multiple seconds and allows you to configure your BGP to minimize traffic loss and improve convergence when a link between the PE and CE router fails.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_best_external_xe.html

BGP VPLS Auto Discovery Support on Route Reflector

On the ASR1000, BGP Route Reflector was enhanced to be able to reflect BGP VPLS prefixes without having VPLS explicitly configured on the route reflector. The route reflector reflects the VPLS prefixes to other provider edge (PE) routers so that the PEs do not need to have a full mesh of BGP sessions.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_int_features_xe.html

Configurable Domain Name Prefix and Suffix Stripping

VPDN Configurable Domain Name Prefix and Suffix Stripping: This feature allows the NAS to be configured to strip prefixes, suffixes, or both from the full username. The reformatted username is then forwarded to the remote AAA server.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/vpdn/configuration/guide/config_aaa_for_vpdn_xe.html

DHCP - DHCPv6 Prefix Delegation RADIUS VSA

DHCP - DHCPv6 Prefix Delegation RADIUS VSA - “When the user requests a prefix from the prefix delegator, typically the NAS, the prefix is allocated using DHCPv6”

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-adsl_dial_xe.html

DHCP Enhancements to Support IPv6 Broadband Deployments

This feature is supported in Cisco IOS XE Release 2.5.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-adsl_dial_xe.html

DHCPv6 Repackaging

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-dhcp_xe.html

DMVPN Manageability Enhancements

DMVPN session manageability was expanded with DMVPN specific commands for debugging, show output, session and counter control, and system log information.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/sec_DMVPN_xe.html

DMVPN: Dynamic tunnels between spokes behind NAT

The DMVPN: Dynamic Tunnels Between Spokes Behind a NAT Device feature allows Next Hop Resolution Protocol (NHRP) spoke-to-spoke tunnels to be built in Dynamic Multipoint Virtual Private Networks (DMVPNs), even if one or more spokes is behind a Network Address Translation (NAT) device.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-3s/DMVPN_Dynamic_Tunnels_Between_Spokes_Behind_a_NAT_Device.html

Dynamic Subscriber Bandwidth Selection

This feature enables wholesale service providers to sell different classes of service to retail service providers by controlling bandwidth at the ATM virtual circuit (VC) level. ATM quality of service (QoS) parameters from the subscriber domain are applied to the ATM PVC on which a PPPoE or PPPoA session is established.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_con_sub_bdwth_xe.html

EtherChannel Min-Links

The EtherChannel Min-Links feature allows a port channel to be shut down when the number of active links falls below the minimum threshold.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/cether/configuration/guide/ce_lnkbndl_xe.html

Firewall - VRF-aware ALG support

VRF-aware ALG support allows ALG to extract the correct IP-address and VRF-id from cached memory when creating ALG tokens.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/sec_data_plane/configuration/guide/sec_vrf_aware_fwall_xe.html

Flow Based Per Port Channel Load Balancing

The Flow-Based Per Port-Channel Load Balancing feature allows different flows of traffic over a Gigabit EtherChannel (GEC) interface to be identified based on the packet header and then mapped to the different member links of the port channel. You can apply flow-based load balancing or VLAN-manual load balancing to specific port channels.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/lanswitch/configuration/guide/lsw_cfg_flwload_xe.html

IEEE 802.3ad - Faster Link Switchover Time

The IEEE 802.3ad Faster Link Switchover Time feature provides a link failover time of 250 milliseconds or less and a maximum link failover time of 2 seconds. Also, port channels remain in the LINK_UP state to eliminate reconvergence by the Spanning-Tree Protocol.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/cether/configuration/guide/ce_lnkbndl_xe.html

IEEE 802.3ad MIB

The IEEE 802.3ad Link Aggregation Control Protocol (LACP) enables the bundling of physical interfaces on a physical device to achieve more bandwidth than is available using a single interface. The LAG MIB supports the management of interfaces and ports that are part of an LACP port channel and is accessed by a Simple Network Management Protocol (SNMP) manager application.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/cether/configuration/guide/ce_lacpmib_xe.html

IPv6 Access Services: AAA Support for Cisco VSA IPv6 Attributes

Vendor-specific attributes (VSAs) were developed to support AAA for IPv6

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-adsl_dial_xe.html

IPv6 Access Services: AAA Support for RFC 3162 IPv6 RADIUS Attributes

The AAA attributes for IPv6 are compliant with RFC 3162 and require a RADIUS server capable of supporting RFC 3162.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-adsl_dial_xe.html

IPv6 Access Services: PPPoA

ADSL and dial deployment is available for interfaces with PPP encapsulation enabled, including PPPoA.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-adsl_dial_xe.html

IPv6 Access Services: PPPoE

ADSL and dial deployment is available for interfaces with PPP encapsulation enabled, including PPPoE.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-adsl_dial_xe.html

IPv6 Access Services: Stateless DHCPv6

The stateless DHCPv6 feature allows DHCPv6 to be used for configuring a node with parameters that do not require a server to maintain any dynamic state for the node.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-dhcp_xe.html

ISG:AAA Wireless Enhancements

The ISG: AAA Wireless Enhancements feature enhances ISG Radius proxy functionality to provide additional support for mobile wireless environments. It includes changes to RADIUS attribute 31 processing.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_radius_proxy_xe.html

ISG:Accounting: Prepaid

The ISG:Accounting: Prepaid feature supports ISG prepaid billing and allows ISG to check a subscriber's available credit to determine whether to allow the subscriber access to a service and how long the access can last. ISG supports volume-based and time-based prepaid billing.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_radius_proxy_xe.html

ISG:Authentication:Radius Proxy WiMax Enhancements

The ISG:Authentication:Radius Proxy WiMax Enhancements feature enhances ISG Radius proxy to provide additional support for WiMax broadband environments.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_radius_proxy_xe.html

ISG:Instrumentation:DHCP Lease Query Support

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_acess_sub_sessns_xe.html

ISG:Policy Control:Differentiated Initial Policy Control

The ISG:Policy Control:Differentiated Initial Policy Control feature provides minimal or temporary network access to the subscribers when the RADIUS servers are down or cannot be accessed because of network issues.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_cntrl_policies_xe.html

ISG:Session: Creation: Interface IP Session: L2

The ISG:Session: Creation: Interface IP Session: L2 feature provides the ability to create Layer 2 IP Sessions for ISG for an entire interface or subinterface.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_acess_sub_sessns_xe.html

ISG:Session: Creation: Interface IP Session: L3

The ISG:Session: Creation: Interface IP Session: L3 feature provides the ability to create Layer 3 IP Sessions for ISG for an entire interface or subinterface.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_acess_sub_sessns_xe.html

ISG:Session:Multicast:Coexistance

The ISG Session Multicast Coexistence feature introduces the ability to host all the subscribers and services (data and multicast) on the same VLAN by enabling multicast and IP sessions to coexist on the same subinterface for Cisco 1000 series routers.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_acess_sub_sessns_xe.html

ISG:Session:Static Session Creation

The ISG Static Session Creation feature enables administrator initiated static IP sessions.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_acess_sub_sessns_xe.html

ISSU - Multicast MPLS VPN

This feature is supported in Cisco IOS XE Release 2.5.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ha/configuration/guide/ha-inserv_updg_xe.html

ISSU – PPPoEoA

The Cisco IOS Broadband High Availability Stateful Switchover feature provides the capability for dual Route Processor systems to support stateful switchover of PPPoX sessions and allow applications and features to maintain state while system control and routing protocol execution is transferred between an active and a standby processor.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_ha_svc_sw_up_xe.html

Layer 2 Local Switching - Same-Port Switching for Ethernet VLAN

Note The Layer 2 Local Switching - Same-Port Switching for Ethernet VLAN feature allows you to switch Layer 2 data between two interfaces on the same router, and in some cases to switch Layer 2 data between two circuits on the same interface port.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/wan_lserv/configuration/xe-3s/wan-l2-lcl-swng-xe.html

Layer 2 Local Switching: Ethernet to VLAN

Note The Layer 2 Local Switching: Ethernet to VLAN feature allows you to switch Layer 2 data between two interfaces on the same router, and in some cases to switch Layer 2 data between two circuits on the same interface port.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/wan/configuration/guide/wan_l2_lcl_swng_xe.html

Link Aggregation Control Protocol (LACP) (802.3ad) for Gigabit Interfaces

The LACP (802.3ad) for Gigabit Interfaces feature bundles individual Gigabit Ethernet links into a single logical link that provides the aggregate bandwidth of up to four physical links.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/cether/configuration/guide/ce_lnkbndl_xe.html

Local Template-Based ATM PVC Provisioning

The Local Template-Based ATM Provisioning feature enables ATM permanent virtual circuits (PVCs) to be provisioned automatically as needed from a local configuration. ATM PVC autoprovisioning can be configured on a PVC, an ATM PVC range, or a VC class. If a VC class configured with ATM PVC autoprovisioning is assigned to an interface, all the PVCs on that interface will be autoprovisioned; this configuration is sometimes referred to as an infinite range.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/atm/configuration/guide/atm_pvc_prov_xe.html

MPLS VPN Half Duplex VRF (HDVRF)

This feature ensures that VPN clients that connect to the same PE router at the edge of the MPLS VPN use the hub site to communicate.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_vpn_half_dup_vrf_xe.html

MSDP MD5 password authentication

The MSDP MD5 password authentication feature is an enhancement to support MD5 signature protection on a TCP connection between two MSDP peers. This feature provides added security by protecting MSDP against the threat of spoofed TCP segments being introduced into the TCP connection stream.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipmulti/configuration/guide/imc_msdp_im_pim_sm_xe.html

Multicast VPN Extranet Support

The Multicast VPN Extranet Support feature enables service providers to distribute IP multicast content originated from one enterprise site to other enterprise sites. This feature enables service providers to offer the next generation of flexible extranet services, helping to enable business partnerships between different enterprise VPN customers

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipmulti/configuration/guide/imc_mc_vpn_extranet_xe.html

Multicast VPN Extranet VRF Select

The Multicast VPN Extranet VRF Select feature provides the capability for RPF lookups to be performed to the same source address in different VRFs using the group address as the VRF selector. This feature enhances extranet MVPNs by enabling service providers to distribute content streams coming in from different MVPNs and redistributing them from there.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipmulti/configuration/guide/imc_mc_vpn_extranet_xe.html

Multicast VPN Inter-AS Support

The Multicast VPN Inter-AS support feature enables MDTs used for MVPNs to span multiple autonomous systems. Benefits include increased multicast coverage to customers that require multicast to span multiple service providers in an MPLS Layer 3 VPN service with the flexibility to support all options described in RFC 4364. Additionally, the Multicast VPN Inter-AS Support feature may be used to consolidate an existing MVPN service with another MVPN service, such as the case with a company merger or acquisition

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipmulti/configuration/guide/imc_cfg_mc_vpn_sup_xe.html

Multicast VPN MIB

The Multicast VPN MIB feature introduces the capability for SNMP monitoring of an MVPN using the MVPN MIB (CISCO-MVPN-MIB).

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipmulti/configuration/guide/imc_vpn_mib_xe.html

Multicast-VPN: Multicast Support for MPLS VPN

The Multicast VPN feature provides the ability to support multicast over a Layer 3 Virtual Private Network (VPN). As enterprises extend the reach of their multicast applications, service providers can accommodate these enterprises over their Multiprotocol Label Switching (MPLS) core network. IP multicast is used to stream video, voice, and data to an MPLS VPN network core.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipmulti/configuration/guide/imc_cfg_mc_vpn_xe.html

NAT - VRF aware NAT for MPLS/VPN

Enables multiple Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) to be configured to work together on a single device. NAT can determine which MPLS VPN it receives IP traffic from even if the MPLS VPNs are all using the same IP addressing scheme. This enhancement enables multiple MPLS VPN customers to share services while ensuring that each MPLS VPN is completely separate from the other.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipaddr/configuration/guide/iadnat_mpls_vpns_xe.html

NAT - VRF-aware ALG support

Enables NAT to support virtual routing and forwarding (VRF) for protocols that require an application level gateway (ALG), such as SIP, H.323, and SCCP/Skinny.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipaddr/configuration/guide/iadnat_applvlgw_xe.html

NBAR PDLM supported in ASR1000 Release 5

Network-Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications. When NBAR recognizes and classifies a protocol or application, the network can be configured to apply the appropriate quality of service (QoS) for that application or traffic with that protocol.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/clsfy_traffic_nbar_xe.html

NHRP - CEF rewrite for DMVPN Phase 3 Networks

Routers in a Dynamic Multipoint VPN (DMVPN) network can use the Next Hop Resolution Protocol (NHRP) to discover the addresses of other routers and networks behind those routers that are connected to a DMVPN nonbroadcast multiaccess (NBMA) network. NHRP provides a solution that alleviates NBMA network problems, such as hub failure, decreased reliability, and complex configurations.

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nhrp/configuration/xe-3s/Shortcut_Switching_Enhancements_for_NHRP_in_DMVPN_Networks.html

NHRP MIB for DMVPN Networks

The Cisco NHRP MIB feature introduces support for the NHRP MIB, which helps to manage and monitor Next Hop Resolution.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/sec_dmvpn_nhrp_mib_xe.html

NSF/SSO - Multicast MPLS VPN

This feature is supported in Cisco IOS XE Release 2.5.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ha/configuration/guide/ha-nonstp_fwdg_xe.html

http://www.cisco.com/en/US/docs/ios/ios_xe/ha/configuration/guide/ha-stfl_swovr_xe.html

PPP Enhancement for Broadband IPv6

This feature is supported in Cisco IOS XE Release 2.5.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-adsl_dial_xe.html

PPP Session Queueing on ATM VC

PPP Session Queuing on ATM Virtual Circuits (VCs) enables you to shape and queue PPP over Ethernet over ATM (PPPoEoA) sessions to a user specified rate.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/ppp_ses_que_atm_vc_xe.html

PPPoE Connection Throttling

PPP over Ethernet (PPPoE) profiles contain configuration information for a group of PPPoE sessions. Multiple PPPoE profiles can be defined for a device, allowing different virtual templates and other PPPoE configuration parameters to be assigned to different PPP interfaces, VLANs, and ATM PVCs that are used in supporting broadband access aggregation of PPPoE sessions.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_pppoe_baa_xe.html

PPPoE on ATM

This feature module describes the PPP over Ethernet (PPPoE) on ATM feature. The PPPoE on ATM feature provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_ppoe_atm_xe.html

PPPoE Session Count MIB

The PPPoE Session Count Management Information Base feature provides the ability to use Simple Network Management Protocol (SNMP) to monitor in real time the number of PPP over Ethernet (PPPoE) sessions configured on permanent virtual circuits (PVCs) and on a router. This MIB also supports two SNMP traps that generate notification messages when a PPPoE session-count threshold is reached on any PVC or on the router.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_mon_pppoe_snmp_xe.html

QoS: QoS support for GRE/sVTI Tunnel

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_a1.html

QoS: Shape Average Percent CLI

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_a1.html

Service Advertisement Framework (SAF)

As the variety and number of network services grows, providing timely and reliable awareness of these services starts to play a more significant role in increasing productivity and efficiency. As networks grow so too do the services offered by the devices on these networks. Protocols responsible for the service advertisement need to scale to handle this increased load. This feature, Service Advertisement Framework (SAF) provides that function.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/saf/configuration/guide/XE_saf_cg.html

Sharing IPSec with Tunnel Protection

The Sharing IPsec with Tunnel Protection feature allows an IP Security (IPsec) security association database (SADB) to be shared between two or more Generic Routing Encapsulation (GRE) tunnel interfaces, when tunnel protection is used.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-3s/Sharing_IPSec_with_Tunnel_Protection.html

SSO - LACP

The SSO – LACP feature supports stateful switchover (SSO), in service software upgrade (ISSU), Cisco nonstop forwarding (NSF),

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/cether/configuration/guide/ce_lnkbndl_xe.html

SSO - PPPoE IPv6

This feature is supported in Cisco IOS XE Release 2.5

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-adsl_dial_xe.html

SSO - PPPoEoA

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/bbdsl/configuration/xe-3s/bba-ha-stfl-swovr-xe.html

VRF Aware Cisco IOS Firewall

VRF Aware Cisco IOS Firewall applies Cisco IOS Firewall functionality to VRF interfaces when the firewall is configured on an SP or large enterprise edge router. SPs can provide managed services to small and medium business markets.

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/sec_data_plane/configuration/guide/sec_vrf_aware_fwall_xe.html

Cisco Unified Border Element (Enterprise)

The Cisco Unified Border Element (Enterprise) on the ASR1000 brings a scalable Cisco UBE (Enterprise) options for enterprise customers. Running as a process on the ASR1000 and utilizing the high speed RTP packet processing path, The primary customers are ones who are consolidating TDM trunks. This release focuses on the initial set of functionality completed for SIP Trunks for PSTN access from Service Providers.

The following Cisco Unified Border (Enterprise) features were introduced in Cisco IOS XE Release 2.5.0:

- Configurable SIP Parameter Modification
- DTMF Events Through SIP Signaling
- Enhanced SIP REFER
- H.323 to SIP Supplementary Feature Interworking for Session Border Controller (SBC)
- iLBC Support for SIP and H.323
- IP-IP Gateway for H323 Call Manager to H323 Service Provider Connectivity
- IP-to-IP Gateway: SIP-SIP Basic Functionality
- SIP - Ability to Send a SIP Registration Message on a Border Element
- SIP - Configurable Hostname in Locally Generated SIP Headers
- SIP - Core SIP Technology Enhancements
- SIP - DNS SRV RFC2782 Compliance
- SIP - Enhanced 180 Provisional Response Handling
- SIP - Gateway Support for the Bind Command
- SIP - INFO Method for DTMF Tone Generation

- SIP - Session Initiation Protocol for VoIP
- SIP - Session Timer Support
- SIP - SIP Basic Feature Functionality for Session Border Controller (SBC)
- SIP - SIP Extended Feature Functionality for Session Border Controller (SBC)
- SIP - SIP GW Session Timer Support
- SIP - Stack Support of TLS
- SIP - Support for SESSION REFRESH with reINVITEs
- SIP and TEL URL Support
- SIP to SIP Supplementary Services for Session Border Controller (SBC)
- SIP:SIP Support for Options
- Support for negotiation of an audio codec from a list of codecs on each leg of a SIP-SIP call on the Cisco Unified Border Element
- 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:

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/config_library/xe-3s/cube-xe-3s-library.html

Cisco Unified Border Element (SP Edition)

The following Cisco Unified Border Element (SP Edition) features were introduced in Cisco IOS XE Release 2.5.0:

- Call duration monitoring
- CDR:Support for CDR Media information
- CDR:Granular Timestamp Support
- H323:H.245 address in Call PROC
- H323:H.323 Registration with Multiple Gatekeepers
- H323:H.323 Slow start to H.323 Fast start Interop
- H323:H.323 Video codec support (H.261, H.263, H.264)
- H.323:In call facility pass through
- H323:Interop with Cisco H.323 gatekeeper
- H323:ITU H.323v4: Packet-Based Multimedia Communications System
- H323:Multiple TCP for H.323
- IMS:Support for Authentication via AKA
- Interop:Support interworking like CCM-SBC-CME topology
- Interworking:CCM-H.323 Slow-start to Fast-start
- Interworking:H.323 - SIP Cause code Mapping
- Interworking:H.323 and SIP interop services
- Interworking:H.323 and SIP Message Translation
- Interworking:H.323 Fast Start Call to SIP call

- Interworking:H.323 Slow Start Calls to SIP calls
- Interworking:H.323 to SIP Support for Emergency calls
- Interworking:H.323/SIP Call Routing
- Interworking:H.323-H.323 Interworking-basic calls
- Interworking:SIP to H.323 Fast Start
- Interworking:T.38 with H.323-H.323 and SIP-H.323.
- Media:Fax/Modem Upspeed Support
- Media:SBC will support Pass through Codec Types
- Media:Transcoding:For external media-server SBC shall work with MGX 8880 Media server.
- Media:Transcoding:SBC shall support external Media Server
- Signaling congestion handling enhancement
- SIP: Ability to Insert Firewall Parameter in SIP Contact Header
- SIP:Ability to adjust "b="""command in SIP INVITE"
- SIP:Call forking
- SIP:Call Park
- SIP:Contact Username Passthrough (non-IMS case)
- SIP:Customizable Late to Early Offer
- SIP:Find Me
- SIP:Instant Messaging and SIMPLE
- SIP:Interoperability for INVITE authentication
- SIP:IP - FQDN URI translation
- SIP:Regular Expression Based Routing
- SIP:SDP media line removal
- SIP:SIP - Specific Event Notification
- SIP:SIP Header Manipulation with Regular Expression/Privacy
- SIP:SIP trunk-group ID routing
- SIP:Support for “Supported: Path” under REGISTER request
- SIP:Support for IP Realm
- SIP:Support for P-KT-UE-IP support
- SIP:Support for PRACK/100rel interworking
- SIP:Support for P-visited-network-ID
- SIP:Support for Softswitch Registration Timer Shielding
- Support for P-called Party Identifier, P-Associated URI (RFC3445)
- Support for Subscriber Policy

For information about these Cisco Unified Border Element (SP Edition) features, see the following documents:

Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/2_xe/sbcu_2_xe_book.html

Cisco Unified Border Element (SP Edition) Command Reference: Unified Model

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

New Hardware Features in Cisco IOS XE Release 2.4.4

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.4.4.

New Software Features in Cisco IOS XE Release 2.4.4

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.4.4.

New Hardware Features in Cisco IOS XE Release 2.4.3

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.4.3.

New Software Features in Cisco IOS XE Release 2.4.3

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.4.3.

New Hardware Features in Cisco IOS XE Release 2.4.2t

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.4.2t.

New Software Features in Cisco IOS XE Release 2.4.2t

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.4.2t.

New Hardware Features in Cisco IOS XE Release 2.4.2

The following hardware features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.4.2:

Cisco ASR 1002 Router

The Cisco +24V DC power supply supports the Cisco ASR 1002 Router with Cisco IOS XE 2.4.2 and later. The Cisco ASR 1002 Router with the new +24V DC power supply is targeted in markets where 24V DC power is required, including, but not limited to, wireless/mobility providers cell-sites.

For information about the Cisco ASR 1002 Router and +24V DC power supply, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide:

http://www.cisco.com/en/US/docs/routers/asr1000/install/guide/asr1routers/asr1higV8.html

and Cisco ASR 1002 Quick Start Guide

http://www.cisco.com/en/US/docs/routers/asr1000/quick/start/guide/asr1_qs2.html

New Software Features in Cisco IOS XE Release 2.4.2

This section lists new and changed features in Cisco IOS XE Release 2.4.2. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS XE Release 2.4.2:

NAT - Forced Clear of Dynamic NAT Half Entries

Provides an optional keyword (forced) to the existing command clear ip nat translations that enable users to clear the NAT table of active dynamic half entries that have existing children translations.

For more information on NAT -Forced Clear of Dynamic Half Entries, see the following document:

https://www.cisco.com/en/US/docs/ios/ios_xe/ipaddr/configuration/guide/iad_monmain_nat_xe.html

New Hardware Features in Cisco IOS XE Release 2.4.1

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.4.1.

New Software Features in Cisco IOS XE Release 2.4.1

This section lists new and changed features in Cisco IOS XE Release 2.4.1. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS XE Release 2.4.1.

- IPv6 IPSec Static Virtual Interface, page 71
- IPSec QoS Group-Based LLQ QoS, page 71
- ALG Support for SIP T.38 Fax Relay over IP, page 71

- ISIS Support for IPv6, page 71

IPv6 IPSec Static Virtual Interface

Static Virtual Tunnel Interface (SVTI) configurations can be used for site-to-site connectivity in which a tunnel provides always-on access between two sites. The advantage of using SVTIs as opposed to map configurations is that users can enable dynamic routing protocols on the tunnel interface without the extra 24 bytes required for GRE headers, thus reducing the bandwidth for sending encrypted data.

For more information on SVTIs, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-ipsec_xe.html

IPSec QoS Group-Based LLQ QoS

A limitation exists when IPSec and QoS are configured on an interface. IPSec uses the egress QoS policy to determine if a packet is a high priority packet before it enqueues it in a low latency queue (LLQ) of the crypto processor. For tunnel interfaces when the QoS policy is applied to the egress physical interface, Tunnel Protection is applied on the tunnel interface, and IPSec cannot determine if the packet is a high priority packet. In this scenario, high priority packets are queued to the default queue—increasing latency and traffic loss during oversubscription.

Starting with Cisco IOS XE Release 2.4.1, QoS group-based LLQ for IPSec provides LLQ functionality before crypto for the limitation described earlier. The idea is to use QoS groups to identify high priority traffic in the IPSec module. Packets are marked with a QoS group at the ingress interface. The user designates certain QoS groups to be used as high priority before crypto.

A new IOS XE command allows the user to configure certain QoS groups as high priority for IPSec:

[**no**] **platform ipsec llq qos-group** *group_num*

This command specifies that packets with QoS group *group_num* (allowed range 1 to 99) are to be treated as high priority packets before crypto and, therefore, are queued into a LLQ before reaching the crypto processor.

ALG Support for SIP T.38 Fax Relay over IP

The SIP Application Layer Gateway has been enhanced to provide NAT and Firewall ALG support for T.38 Fax Relay over IP.

ISIS Support for IPv6

Intermediate System (IS-IS) has been enhanced to provide Internet Protocol version 6 (IPv6).

New Hardware Features in Cisco IOS XE Release 2.4.0

The following new hardware features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.4.0:

Cisco ASR 1002-Fixed Router

The Cisco ASR 1002-Fixed (Cisco ASR 1002-F) Router is the smallest of the Cisco ASR 1000 Series Aggregation Services Routers and supports all the general-purpose routing and security features of the Cisco ASR 1002 Router.

The Cisco ASR 1002-F Router uses the same internal control and data-plane architecture as the Cisco ASR 1002 router with the following variations:

- Has all integrated components: an integrated route processor (Cisco ASR1000-RP1), an integrated embedded services processor (2.5-Gbps Cisco ASR 1000 Series ESP), and an integrated 4xGE SPA interface (Cisco ASR1000-SIP10)
- Supports 2.5 GB of system bandwidth
- Is supported only with Cisco IOS XE Release 2.4.0 and later releases

For information about the Cisco ASR 1002-F Router, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/install/guide/asr1routers/asr1higV8.html

Cisco ASR 1002-F Quick Start Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/quick/start/guide/asr1_qs2F.html

New Shared Port Adapters

Cisco IOS XE Release 2.4.0 introduces support for the following new shared port adapters (SPAs):

POS SPAs

- 8-Port OC-3 POS SPA (SPA-8XOC3-POS)
- 2-Port, 4-Port, and 8-Port OC-12 POS SPAs (SPA-2XOC12-POS, SPA-4XOC12-POS, and SPA-8X0C-12-POS)
- 1-Port OC-48 POS SPA (SPA-1XOC48POS/RPR)
- 1-Port OC-192 POS SPA (SPA-OC192POS-XFP)

Services SPA

- Cisco WebEx Node for ASR 1000 Series (SPA-WMA-K9)

  The Cisco WebEx Node for ASR 1000 Series is a full-height SPA designed to run an application which is part of the WebEx MediaTone network management application. The Cisco WebEx Node for ASR 1000 Series improves the functionality of WebEx meeting services by adding the meeting servers into the SPA itself. This technology provides the following advantages:

  - Improves performance for users inside the company firewall.
  - Reduces the bandwidth going out of company firewall (to the WebEx MediaTone network).
  - Provides better security by reducing traffic outside the company.

By moving the switching components of the WebEx Collaboration Cloud into the Cisco WebEx Node for ASR 1000 Series, the WebEx clients in the enterprise network need only connect to the Cisco WebEx Node for ASR 1000 Series. This reduces the traffic between the enterprise network and the WebEx MediaTone network, greatly reducing the customer's Internet bandwidth requirements.

Each Cisco WebEx Node for ASR 1000 Series can be configured to perform either web conferencing or voice and video conferencing, but not both features at the same time. Each Cisco WebEx Node for ASR 1000 Series uses the same software package that includes both features; the conferencing feature that actually runs on each SPA is determined by the WebEx Service Plan the customer has purchased. The WebEx MediaTone network retains the Cisco WebEx Node for ASR 1000 Series configuration files that the SPA retrieves each time the SPA boots. Multiple Cisco WebEx Nodes for ASR 1000 Series can be installed on the same Cisco ASR 1000 Series Router chassis to increase the conferencing performance or to provide conferencing coverage for both web and voice and video sessions.

For information about the SPAs supported on the Cisco ASR 1000 Series Routers, see the following documents:

- *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide* at the following location:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/ASR1000/asr_sip_spa_hw.html

- *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide* at the following location:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ASR1000/ASRspasw.html

New Software Features in Cisco IOS XE Release 2.4.0

This section lists new and changed features in Cisco IOS XE Release 2.4.0. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS XE Release 2.4.0.

- IS-IS Support for IPv6
- 3 Level Egress QoS Policy
- 802.1P CoS Bit Set for PPP and PPPoE Control Frames
- AAA Interim Accounting
- ACL—Template ACL/12 Bit ACE
- ANCP (Access Node Control Protocol)
- ANCP Phase 2.5
- Any Transport over MPLS (AToM): Ethernet over MPLS (EoMPLS)
- Any Transport over MPLS (AToM): Ethernet over MPLS: Port Mode (EoMPLS)
- Any Transport over MPLS (AToM): Remote Ethernet Port Shutdown
- Any Transport over MPLS— Ethernet over MPLS Enhancements: Fast Reroute
- Asynchronous Rotary Line Queuing
- Byte-Based Weighted Random Early Detection

- Cache Control Enhancements for Certification Revocation Lists
- Certificate—Complete Chain Validation
- Cisco IOS SHA2 Support
- Cisco Unified Border Element (SP Edition)
- Class-Based QoS MIB (CBQoSMIB) Enhancements
- CoA—Multi-Service Activation/Deactivation in Single mMessage
- Connect-info RADIUS Attribute 77—Configurable ASCII String
- DHCP Server Radius Proxy
- Enabling ISG to Interact with External Policy Servers
- Etherchannel Flow Based Limited 1:1 Redundancy
- Ethernet Overhead Accounting
- Firewall—SIP ALG—Extended Methods
- Firewall—SIP ALG—Extended Methods
- H.323 RAS Support in IOS Firewall
- IEEE 802.1Q Tunneling (QinQ) for AToMLawful Intercept
- IEEE 802.3ad Link Aggregation (LACP)
- Integrated Session Border Controller
- Interactive OAM and Scaling Improvements
- IP over IPv6 Tunnels
- IPsec Usability Enhancements
- IPv6 Multicast: Bootstrap Router (BSR)
- IPv6 Multicast: IPv6 BSR—Ability to Configure RP Mapping
- IPv6 Multicast: IPv6 BSR Bidirectional Support
- IPv6 Multicast: PIM Sparse Mode (PIM-SM)
- IPv6 Multicast: Routable Address Hello Option
- ISG: Accounting: Per-Service Accounting
- ISG: Policy Control: Policy Server: Multi-Service Activation in access-accept Message
- ISG: Policy Control: Policy Server: RADIUS-Based Policing
- L2TP Forwarding of PPPoE Tag Information
- L2VPN Interworking—Ethernet to VLAN Interworking
- L2VPN Pseudowire Redundancy: Multiple Backup Pseudowires
- L2VPN Pseudowire Switching
- Lawful Intercept
- Layer 2 VPN (L2 VPN): Syslog, SNMP Trap, and show Command Enhancements for AToM and L2TPv3
- MCP GEC with QoS on memberlink
- Modified LNS Dead-Cache Handling
- MQC—Traffic Shaping Overhead Accounting for ATM

- NAT—NetMeeting Directory (LDAP) ALG Support
- NAT SCCP Video Support
- NAT—SIP ALG—Extended Methods
- NAT Support of H.323v2 RAS
- NSF/SSO—Ethernet to Ethernet VLAN Interworking
- OCSP—Server Certification from Alternate Hierarchy
- Parameterization for ACL and Layer 4 Redirect
- Parameterization of QoS ACL
- Per Subinterface MTU for Ethernet over MPLS (EoMPLS)
- PKI—CLI to Control Certificate Revocation List (CRL) Cache
- PPPoE Service Selection
- PPPoE Session Limit
- PPPoE Smart Server Selection
- PPPoE VLAN Session Throttling
- Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services
- QoS: CBQoSMIB Index Enhancements
- RADIUS-Based Lawful Intercept
- RADIUS-Based Policing Attribute Modifications
- RADIUS—CLI to Prevent Sending of Access Request with Blank Username
- RSA 4096-Bit Key Generation in Software Crypto Engine Support
- SCCP for Video
- SSHv2 Enhancements
- VLAN ID Rewrite
- VPDN LNS Address Checking
- VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP
- VRF Aware LI (Lawful Intercept)

IS-IS Support for IPv6

Intermediate System-to-Intermediate System (IS-IS) has been enhanced to support Internet Protocol version 6 (IPv6). For more information on implementing IS-IS support, see the *Cisco IOS XE IPv6 Configuration Guide, Release 2* at the following URL:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-is-is_xe_ps9587_TSD_Products_Configuration_Guide_Chapter.html

3 Level Egress QoS Policy

The 3 Level Egress QoS Policy feature allows 3 level hierarchical QoS policies to be applied as an egress service per physical interface or per VLAN (GE) or per subinterface (FR or serial).

At the top level, only class-default with shaping can be configured.

At the medium level, user defined classes can be configured where for each user defined class following can be applied:

- Bandwidth Remaining (BR): either as Bandwidth Remaining Ratio (BRR) or Bandwidth Remaining Percentage (BRP) or
- shaping or
- priority (conditional or unconditional policer)

All of the three items listed above can be configured concurrently with WRED.

At the bottom level, user defined classes can be configured where for each user defined class either policing or marking can be applied.

802.1P CoS Bit Set for PPP and PPPoE Control Frames

The 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature provides the ability to set user priority bits in the IEEE 802.1Q tagged frame to allow traffic prioritization.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_cos_ppp_pppoe_xe.html

AAA Interim Accounting

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_accountg.html

ACL—Template ACL/12 Bit ACE

The Template ACL feature groups ACLs with many common access control elements (ACEs) into a single ACL that saves system resources.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_tmplacl.html

ANCP (Access Node Control Protocol)

The Access Node Control Protocol feature enhances communication between Digital Subscriber Line Access Multiplexers (DSLAMs) and a broadband remote access server (BRAS), enabling the exchange of events, actions, and information requests between the multiplexer end and the server end. As a result, either end can implement appropriate actions.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ancp/configuration/guide/ancp_xe.html

ANCP Phase 2.5

The ANCP Phase 2.5 feature allows multiple services to be activated or deactivated by a single Change of Authorization (CoA) message sent from the policy server.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ancp/configuration/guide/ancp_msad_coa_xe.html

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

The Any Transport over MPLS (AToM): Ethernet over MPLS (EoMPLS) feature allows you to transport Layer 2 Ethernet VLAN packets from various sources over an MPLS backbone. Ethernet over MPLS extends the usability of the MPLS backbone by enabling it to offer Layer 2 services in addition to already existing Layer 3 services.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_any_transport_xe.html

Any Transport over MPLS (AToM): Ethernet over MPLS: Port Mode (EoMPLS)

Ethernet over MPLS (EoMPLS) is the transport of Ethernet frames across an MPLS core. It transports all frames received on a particular Ethernet or virtual LAN (VLAN) segment, regardless of the destination Media Access Control (MAC) information.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_any_transport_xe.html

Any Transport over MPLS (AToM): Remote Ethernet Port Shutdown

The Any Transport over MPLS (AToM): Remote Ethernet Port Shutdown feature allows a service provider edge (PE) router on the local end of an Ethernet over MPLS (EoMPLS) pseudowire to detect a remote link failure and cause the shutdown of the Ethernet port on the local customer edge (CE) router. Because the Ethernet port on the local CE router is shut down, the router does not lose data by continuously sending traffic to the failed remote link.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_any_transport_xe.html

Any Transport over MPLS— Ethernet over MPLS Enhancements: Fast Reroute

The Any Transport over MPLS— Ethernet over MPLS Enhancements: Fast Reroute feature allows AToM to use MPLS traffic engineering (TE) tunnels with fast reroute (FRR) support. This feature enhances FRR functionality for Ethernet over MPLS (EoMPLS).

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_any_transport_xe.html

Asynchronous Rotary Line Queuing

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_asyn_que_role.html

Byte-Based Weighted Random Early Detection

The Byte-Based Weighted Random Early Detection feature extends the functionality of WRED. In previous releases, you specified the WRED actions based on the number of packets. With the Byte-Based WRED, you can specify WRED actions based on the number of bytes.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/fsbyte_xe.html

Cache Control Enhancements for Certification Revocation Lists

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_auth_rev_cert.html

Certificate—Complete Chain Validation

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_auth_rev_cert.html

Cisco IOS SHA2 Support

The Cisco IOS SHA2 Support feature allows the user to specify a cryptographic hash function for Cisco IOS certificate servers and clients. The cryptographic hash functions that can be specified are Message-Digest algorithm 5 (MD5), Secure Hash Algorithm -- SHA-1, SHA-256, SHA-384, or SHA-512.

The following commands were introduced by this feature: **hash (ca-trustpoint)** and **hash (cs-server)**. The **hash (ca-trustpoint)** command sets the hash function for the signature that the Cisco IOS client uses to sign its self-signed certificates. The **hash (cs-server)** command sets the hash function for the signature that the Cisco IOS certificate authority (CA) uses to sign all of the certificates issued by the server.

Cisco Unified Border Element (SP Edition)

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller.

With Cisco IOS XE Release 2.4.0, Cisco Unified Border Element (SP Edition) can operate in two modes or deployment models:

- Unified—In the unified model, both the SBE and DBE logical entities co-exist on the same network element. In this model, the signaling entity controls the media local to the router.
- Distributed—In the distributed model, the SBE and the DBE entities reside on different network elements. Logically, each of the SBE entities controls multiple DBE elements, and each DBE can be controlled by multiple SBE entities.

Note For Cisco IOS XE Release 2.3 and earlier releases of the Integrated Session Border Controller, only DBEs in the distributed model are supported.

In addition to introducing support for the SBC unified model, Cisco IOS XE Release 2.4.0 introduces support for the following Session Border Controller (SBC) features:

- AAA: End Point Authentication
- CAC: Bypass Admission Control for Emergency Calls
- CAC: CAC Enforcement Notification
- CAC: Configurable Rate Limiting
- CAC: DBE Shall Support DSCP Settings
- CAC: Policing and Marking Under SBE Control
- CAC: Policing: Number Analysis: Depending on Destination Adjacency
- CAC: Policing: Per Session Policing
- CAC: Policing: SBC Shall Support Whitelisting and Blacklisting Profiles Based on Request for Methods
- CAC: Policing: BC Shall Support Policy Based Session Routing
- CAC: Priority Handling of Traffic During an Attack or When System's Resources Are Overloaded
- CAC: SBE Shall Support Various CAC Mechanisms
- CDR: 24 hours CDR Buffering
- CDR: Real Time CDRs Can Be Extracted Upon Completion of a Session
- CDR: Send CDR to Radius Server
- Config: ALARM/Statistics
- Config: All Timer Values Should Be Configurable with Default Values
- Config: DBE Shall Provide QoS Statistics to SBE in Realtime upon Call Completion
- Config: DBE Shall Support to Collect Statistics of the Session
- Config: Display Session States in Real-time
- Config: Load Balancing
- Config: Required Debug Commands
- Config: SBE/DBE CLI Consistency
- Config: SBE Shall Support the Ability to Specify QoS for the Session Based QoS Categories
- Config: Shut/No-Shut of SBE/DBE/SBC
- Delta Renegotiation
- DoS: DoS (Denial of Service)
- DoS: Guard Against DoS Attack at Signaling Level
- DoS: Monitoring and Blacklisting Signaling/Media Traffic for a DoS Attack
- DoS: Signaling and Control Packets
- DoS: Media Pinhole Provides an Alert for Packets with Unknown Source Address
- HA: 1:1 Redundancy Support
- HA: 2 Seconds Until New Sessions Can Be Established Following Failover
- HA: Active Session Preservation Across Failover
- HA: Media Path Interruption Should Be Less Than 1 Second During Failover

- IMS: Support for P-CSCF Subscription to Subscriber Registration State
- Interop: Interop with CCM and SIP IP Phones
- Interop: Interop with Cisco SIP Proxy Servers
- Interop: Interop with Telepresence System
- Media: DTMF Interworking Support
- Media: DTMF Support for SIP-Notify
- Media: Fax/Modem Passthrough Support
- Media: Inter-VPN Media Relay Bypass
- Media: Media Packet Updates
- Media: RTCP Processing
- Media: Support DTMF Processing
- Media: Support for RFC 3550 (RTP)
- Media: Support for RFC 3551
- Media: Support for Video Codecs—H.263 and H.264
- Media: Support Media Relay
- Media: VPN Awareness and Translation
- MIB: Support SNMP Call Stats Requirements
- MIB: Support SNMP TRAPS Requirements
- NAPT: NAPT Traversal
- NAT: NAT Traversal
- Option to Use CODEC Instead of Bandwidth-Field for Media Bandwidth Allocation
- Performance: Jitter Measurement
- Performance: Latency Measurement
- QoS: DSCP, Pre/TOS, and MPLS EXO\P Marking for Media, Signaling and Control Traffic
- Radius: Configurable Radius Authentication/Accounting Server Port
- Radius: Support Multiple Radius Servers
- Security: Private Extensions to the SIP for Asserted Identity within Trusted Networks
- Security: Short Term Requirements for Network Asserted Identity
- Security: Support DTLS for SIP Signaling
- Security: Support for SRTP
- Security: Support Multi-VFF Support for SBC
- Security: Support TLS-TLS and TLS-nonTLS Call Support
- Security: TLS Encrypted Signaling Across SP-SP Border
- Security: Transport=TLS parameter in Record Route Headers
- SIP: 3xx Support
- SIP: Allow Fast Register and Softswitch Shielding to Be Configured Independently
- SIP: BYE Storm Pacing
- SIP: Call Forwarding—Busy

- SIP: Call Forwarding—No Answer
- SIP: Call Forwarding—Unconditional
- SIP: Call Hold
- SIP: Call Hold Interworking
- SIP: Call Hold with MOH
- SIP: Call Routing Enhancement
- SIP: Caller-ID and Calling Name Delivery
- SIP: Click To Dial
- SIP: Codec AAC-LD Support
- SIP: Consultation Hold
- SIP: Delayed Media to Early Media Support
- SIP: Delegated Registration
- SIP: Dynamic Route Selection
- SIP: HTTP Digest Authentication
- SIP: Min-SE Support
- SIP: Music On Hold (MOH)
- SIP: MWI (Message Waiting Indicator)
- SIP: Reason Header
- SIP: RFC 3262 PRACK (Provisional Response)
- SIP: RFC 3264 An Offer/Answer Model with the SDP
- SIP: RFC 3892 Referred-By Mechanism
- SIP: RFC2976 SIP INFO method
- SIP: RFC3261
- SIP: session-expire Support
- SIP: SIP Aggregation Registration
- SIP: SIP Header and Value Manipulation
- SIP: SIP Registration Forwarding
- SIP: SIP Session Refreshment with re-INVITE
- SIP: SIP to Tel URI
- SIP: SRTP S-Description Passthrough
- SIP: Support for VPN DNS Resolution
- SIP: Support 100rel in Supported Header
- SIP: Support Fast Registration
- SIP: Support for Diversion Header
- SIP: Support for SIP Date Header
- SIP: Support for SIP JOIN Header
- SIP: Support for SIP Profile for Message Normalization
- SIP: Support TCP/UDP and Interoperability

- SIP: Support Tel URI
- SIP: timer Support
- SIP: Transfer—Attended
- SIP: Transfer—Unattended
- SIP: Transfer—Instant
- SIP: user=phone Parameter
- SIP: Video Support with E.164 and SIP URI
- Support Renegotiated Call Over NAT
- T.38 Passthrough
- Topology-Hiding: Infrastructure and Topology Hiding
- TP Support for Secure Media
- VPN Awareness and Interconnect

For information about these SBC features, see the following documents:

Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/2_xe/sbcu_2_xe_book.html

Note Because the *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model* uses a task-oriented approach to SBC features, each individual feature is not necessarily identified by feature name within the configuration guide.

Cisco Unified Border Element (SP Edition) Command Reference: Unified Model

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

Class-Based QoS MIB (CBQoSMIB) Enhancements

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/cbqos_mib_xe.html

CoA—Multi-Service Activation/Deactivation in Single mMessage

The CoA—Multi-Service Activation/Deactivation in Single mMessage feature allows multiple services to be activated or deactivated by a single Change of Authorization (CoA) message sent from the policy server.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ancp/configuration/guide/ancp_msad_coa_xe.html

Connect-info RADIUS Attribute 77—Configurable ASCII String

The Connect-Info RADIUS Attribute 77 feature enables the network access server (NAS) to report Connect-Info (attribute 77) in RADIUS accounting “start” and “stop” records that are sent to the RADIUS client (dial-in modem). These “start” and “stop” records allow the transmit and receive connection speeds, modulation, and compression to be compared in order to analyze a user session over a dial-in modem where speeds are often different at the end of the connection (after negotiation).

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/sec_user_services/configuration/guide/sec_rad_77_connect_xe.html

DHCP Server Radius Proxy

The Dynamic Host Configuration Protocol (DHCP) Server RADIUS Proxy feature is a RADIUS-based address assignment mechanism in which a DHCP server authorizes remote clients and allocates addresses based on replies from a RADIUS server.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipaddr/configuration/guide/iad_dhcp_rad_proxy_xe.html

Enabling ISG to Interact with External Policy Servers

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/en_isg_ext_plcy_svrs_xe.html

Etherchannel Flow Based Limited 1:1 Redundancy

The EtherChannel Flow-Based Limited 1:1 Redundancy feature provides a way to configure load balancing at the port-channel level based on different flows of traffic. You can identify different flows of traffic based on key fields in the data packet and balance the traffic load according to those traffic flows. To use EtherChannel flow-based limited 1:1 redundancy, you configure an EtherChannel with two ports (one active and one standby). If the active link goes down, the EtherChannel stays up and the system performs fast switchover to the hot-standby link. When the failed link becomes operational again, the EtherChannel performs another fast switchover to revert to the original active link.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/lanswitch/configuration/guide/lsw_cfg_flwbal.html

Ethernet Overhead Accounting

The Ethernet Overhead Accounting feature enables the router to account for downstream Ethernet frame headers when applying shaping to packets.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/eth_overhead_acctng_xe.html

Firewall—SIP ALG—Extended Methods

The Firewall—SIP ALG—Extended Methods feature provides voice security enhancements within the Firewall feature set in Cisco IOS XE software on the Cisco ASR 1000 series routers.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/sec_data_plane/configuration/guide/sec_fw_sip_alg_xe.html

H.323 RAS Support in IOS Firewall

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_h323ras_firewall.html

IEEE 802.1Q Tunneling (QinQ) for AToM

The IEEE 802.1Q Tunneling (QinQ) for AToM feature allows you to configure IEEE 802.1Q Tunneling (QinQ) for AToM. It also permits the rewriting of QinQ tags for Multiple Protocol Label Switching (MPLS) layer 2 VPNs (L2VPNs).

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_qnq_tunneling_atom_xe.html

IEEE 802.3ad Link Aggregation (LACP)

The IEEE 802.3ad Link Aggregation (LACP) feature provides a method for aggregating multiple Ethernet links into a single logical channel based on the IEEE 802.3ad standard. This feature helps improve the cost effectiveness of a device by increasing cumulative bandwidth without necessarily requiring hardware upgrades.

For information about this feature, see the *Configuring IEEE 802.3ad Link Bundlin*g document:

http://www.cisco.com/en/US/docs/ios/ios_xe/cether/configuration/guide/ce_lnkbndl_xe.html

Integrated Session Border Controller

The product formerly known as Integrated Session Border Controller is now known as the Cisco Unified Border Element (SP Edition). For information about this feature, see Cisco Unified Border Element (SP Edition).

Interactive OAM and Scaling Improvements

The Interactive OAM and Scaling Improvements feature adds on-demand ping capability to access node control protocol (ANCP) for operations and troubleshooting.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ancp/configuration/guide/ancp_xe.html

IP over IPv6 Tunnels

For information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-tunnel_xe.html

http://www.cisco.com/en/US/docs/ios/ios_xe/interface/configuration/guide/ir_impl_tun_xe.html

IPsec Usability Enhancements

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ipsec_vpn_status_monitoring.html

IPv6 Multicast: Bootstrap Router (BSR)

If an RP becomes unreachable, the IPv6 Multicast: Bootstrap Router (BSR) feature allows the RP to be detected and the mapping tables modified so that the unreachable RP is no longer used, and the new tables will be rapidly distributed throughout the domain.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html

IPv6 Multicast: IPv6 BSR—Ability to Configure RP Mapping

TheIPv6 Multicast: IPv6 BSR—Ability to Configure RP Mapping feature allows IPv6 multicast routers to be statically configured to announce scope-to-RP mappings directly from the BSR instead of learning them from candidate-RP messages.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html

IPv6 Multicast: IPv6 BSR Bidirectional Support

The IPv6 Multicast: IPv6 BSR Bidirectional Support feature allows bidirectional RPs to be advertised in C-RP messages and bidirectional ranges in the BSM.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html

IPv6 Multicast: PIM Sparse Mode (PIM-SM)

TheIPv6 Multicast: PIM Sparse Mode (PIM-SM) feature uses unicast routing to provide reverse-path information for multicast tree building. PIM-SM is used in a multicast network when relatively few routers are involved in each multicast and these routers do not forward multicast packets for a group, unless there is an explicit request for the traffic.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html

IPv6 Multicast: Routable Address Hello Option

The IPv6 Multicast: Routable Address Hello Option feature adds a PIM hello message option that includes all the addresses on the interface on which the PIM hello message is advertised.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html

ISG: Accounting: Per-Service Accounting

The Intelligent Services Gateway (ISG) Per-Service Accounting feature provides the means to bill for account or service usage. ISG accounting uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based authentication, authorization, and accounting (AAA) or mediation server.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/cfg_isg_acctng_xe.html

ISG: Policy Control: Policy Server: Multi-Service Activation in access-accept Message

The ISG: Policy Control: Policy Server: Multi-Service Activation in access-accept Message feature allows multiple services to be included in a single RADIUS access-accept message.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ancp/configuration/guide/ancp_msa_acc_xe.html

ISG: Policy Control: Policy Server: RADIUS-Based Policing

The RADIUS-Based Policing feature extends Intelligent Services Gateway (ISG) functionality to allow the use of a RADIUS server to provide subscriber policy information.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_rabapol_xe.html

L2TP Forwarding of PPPoE Tag Information

The L2TP Forwarding of PPPoE Tag Information feature allows you to transfer DSL line information from the L2TP Access Concentrator (LAC) to the L2TP Network Server (LNS). Using this feature, you can also override the nas-port-id and/or calling-station-id VSAs on the LNS with the Circuit-ID and Remote-ID VSA respectively.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/vpdn/configuration/guide/config_aaa_for_vpdn_xe.html

L2VPN Interworking—Ethernet to VLAN Interworking

The L2VPN Interworking—Ethernet to VLAN Interworking feature allows disparate attachment circuits to be connected. An interworking function facilitates the translation between the different Layer 2 encapsulations.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_l2vpn_intrntwkg_xe.html

L2VPN Pseudowire Redundancy: Multiple Backup Pseudowires

The L2VPN Pseudowire Redundancy: Multiple Backup Pseudowires feature allows you to configure up to three backup pseudowires to maintain network connectivity if one pseudowire fails.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/wan_l2vpn_pw_red_xe.html

L2VPN Pseudowire Switching

The L2VPN Pseudowire Switching feature extends layer 2 virtual private network (L2VPN) pseudowires across an interautonomous system (inter-AS) boundary or across two separate multiprotocol label switching (MPLS) networks.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_l2vpn_pseudo_swit_xe.html

Lawful Intercept

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_lawful_intercept.html

Layer 2 VPN (L2 VPN): Syslog, SNMP Trap, and show Command Enhancements for AToM and L2TPv3

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_l2_tun_pro_v3.html

MCP GEC with QoS on memberlink

Previously available on only port-channel subinterfaces, QoS can now be applied to the main GigabitEtherChannel (GEC) interface, or memberlink. QoS is applied through policy maps.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/lanswitch/configuration/guide/lsw_cfg_gecqos.html

Modified LNS Dead-Cache Handling

The Modified LNS Dead-Cache Handling feature allows you to display and clear (restart) any Layer 2 Tunnel Protocol (L2TP) Network Server (LNS) entry in a dead-cache (DOWN) state. You can use this feature to generate a Simple Network Management Protocol (SNMP) or system message log (syslog) event when an LNS enters or exits a dead-cache state. Once an LNS exits the dead-cache state, the LNS is able to establish new sessions.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/vpdn/configuration/guide/config_aaa_for_vpdn_xe.html

MQC—Traffic Shaping Overhead Accounting for ATM

The MQC—Traffic Shaping Overhead Accounting for ATM feature enables a broadband aggregation system (BRAS) to account for various encapsulation types when applying QoS functionality to packets.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/overhead_acctng_xe.html

NAT—NetMeeting Directory (LDAP) ALG Support

Cisco IOS XE NAT provides ALG support for NetMeeting directory Lightweight Directory Access Protocol (LDAP) messages.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipaddr/configuration/guide/iadnat_applvlgw_xe.html

NAT SCCP Video Support

Cisco IOS XE NAT provides Skinny Call Control Protocol (SCCP) message translation support.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipaddr/configuration/guide/iadnat_applvlgw_xe.html

NAT—SIP ALG—Extended Methods

Cisco IOS XE NAT supports extended methods for the Session Initiation Protocol (SIP.)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipaddr/configuration/guide/iadnat_applvlgw_xe.html

NAT Support of H.323v2 RAS

Cisco IOS XE NAT supports H.225 and H.245 message types, including those sent in the Registration, Admission, and Status (RAS) protocol.

RAS provides a number of messages that are used by software clients and VoIP devices to register their location, request assistance in call set up, and control bandwidth. The RAS messages are directed toward an H.323 gatekeeper.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipaddr/configuration/guide/iadnat_applvlgw_xe.html

NSF/SSO—Ethernet to Ethernet VLAN Interworking

The NSF/SS0—Ethernet to Ethernet VLAN Interworking features enables stateful switchover (SSO) and nonstop forwarding (NSF) capabilities for Ethernet to VLAN attachment circuits. Changes in the learned MAC address for interworking are reflected on the standby RP so that identical values exist on the Active and Standby RPs.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_trnsprt_mlps_atom_xe.html

OCSP—Server Certification from Alternate Hierarchy

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_auth_rev_cert.html

Parameterization for ACL and Layer 4 Redirect

The Parameterization for ACL and Layer 4 Redirect feature provides parameterization enhancements for access control lists and Layer 4 redirect.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_l4_redirect_xe.html

Parameterization of QoS ACL

The Parameterization of QoS ACL feature provides enhancements for quality of service (QoS) access control lists (ACLs). This feature allows the authentication, authorization, and accounting (AAA) device to dynamically change parameters.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_rabapol_xe.html

Per Subinterface MTU for Ethernet over MPLS (EoMPLS)

The Per Subinterface MTU for Ethernet over MPLS (EoMPLS) feature provides you with the ability to specify maximum transmission unit (MTU) values in xconnect subinterface configuration mode. When you use xconnect subinterface configuration mode to set the MTU value, you establish a pseudowire connection for situations where the interfaces have different MTU values that cannot be changed.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_any_transport_xe.html

PKI—CLI to Control Certificate Revocation List (CRL) Cache

The PKI-CLI to Control Certificate Revocation List (CRL) Cache feature allows the administrator to control the CRL cache size. CRLs are received by Cisco IOS software in Distinguished Encoding Rules (DER) encoded format. Because processing a DER encoded CRL uses CPU memory, Cisco IOS software allows CRLs either to be stored in cache after being processed or to be decoded. Configuring the CRL cache size allows the amount of memory to be decreased (for example, if low memory conditions exist) or to be increased (for example, when a large number of CRLs are being processed), resulting in better performance.

The following commands were introduced or modified by this feature: **crypto pki crl cache** and **show crypto pki crls**. The **crypto pki crl cache** command allows the administrator to set the maximum amount of volatile memory used to cache CRLs. When the **crypto pki crl cache** command is configured, the **show crypto pki crls** command output includes information on the CRL cache size.

PPPoE Service Selection

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_pppoe_baa_xe.html

PPPoE Session Limit

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_limit_legcfg_xe.html

PPPoE Smart Server Selection

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_pppoe_sss_xe.html

PPPoE VLAN Session Throttling

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_pppoe_baa_xe.html

Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services

The Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services feature provides Simple Network Management Protocol (SNMP) support within an Any Transport over Multiprotocol Label Switching (AToM) infrastructure emulating Ethernet, Frame Relay, and ATM services over packet switched networks (PSNs).

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_edge2edge_mibs_xe.html

QoS: CBQoSMIB Index Enhancements

The QoS: CBQoSMIB Index Enhancements feature allows automatic inclusion of downstream Ethernet frame headers in shaped rate

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/cbqos_mib_xe.html

RADIUS-Based Lawful Intercept

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_lawful_intercept.html

RADIUS-Based Policing Attribute Modifications

The RADIUS-Based Policing Attribute Modifications feature allows the RADIUS server to communicate with the Intelligent Services Gateway (ISG) by embedding specific attributes in Access-Accept and CoA messages. RADIUS-based shaping and policing employs this exchange of attributes to activate and deactivate services, and to modify the active quality of service (QoS) policy applied to a session.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/isg/configuration/guide/isg_rabapol_xe.html

RADIUS—CLI to Prevent Sending of Access Request with Blank Username

The **aaa authentication suppress null-username** command is used to provide the ability to prevent an Access Request with a blank username from being sent to the RADIUS server. This functionality ensures that unnecessary RADIUS server interaction is avoided, and RADIUS logs are kept short.

For information about this feature, see the “Preventing an Access Request with a Blank Username from Being Sent to the RADIUS Server” subsection in following document:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authentifcn.html

RSA 4096-Bit Key Generation in Software Crypto Engine Support

The RSA 4096-Bit Key Generation in Software Crypto Engine Support feature increases the maximum RSA key size from 2048 bits to 4096 bits for private key operations.

SCCP for Video

The SCCP for Video feature enables Cisco Firewalls to inspect Skinny control packets that are exchanged between a Skinny client and the Cisco Call Manager.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/sec_data_plane/configuration/guide/sec_zone_polcy_firew_xe.html

SSHv2 Enhancements

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_shell_v2.html

VLAN ID Rewrite

The VLAN ID Rewrite feature enables you to use VLAN interfaces with different VLAN IDs at both ends of the tunnel.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_any_transport_xe.html

VPDN LNS Address Checking

The VPDN LNS Address Checking feature allows an L2TP Access Concentrator (LAC) to check the IP address of the L2TP Network Server (LNS) sending traffic to it during the setup of an L2TP tunnel, thus providing a check for uplink and downlink traffic arriving from different interfaces.

The benefit of the LNS Address Checking feature is avoiding the loss of revenue from users sending back traffic through an alternate network.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/vpdn/configuration/guide/config_aaa_for_vpdn_xe.html

VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_per_vrf_aaa.html

VRF Aware LI (Lawful Intercept)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_lawful_intercept.html

New Hardware Features in Cisco IOS XE Release 2.3.2

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.3.2.

New Software Features in Cisco IOS XE Release 2.3.2

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.3.2.

New Hardware Features in Cisco IOS XE Release 2.3.1

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.3.1.

New Software Features in Cisco IOS XE Release 2.3.1

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.3.1.

New Hardware Features in Cisco IOS XE Release 2.3.0

The following new hardware features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.3.0:

- New Cisco ASR 1000 Route Processor
- New Shared Port Adapters

New Cisco ASR 1000 Route Processor

Cisco IOS XE Release 2.3.0 introduces support for the following new Route Processor (RP):

Cisco ASR 1000 Series Route Processor 2

The Cisco ASR 1000 Series Route Processor 2 (Cisco ASR1000-RP2) is the second-generation route processor for the Cisco ASR 1000 Series Aggregation Services Router. The Cisco ASR1000-RP2 provides advanced routing capabilities, monitors and manages the other components of the Cisco ASR 1000 Series Aggregation Services Router, and provides a processing engine for integrated applications. In addition to the current route processing features and benefits of the Cisco ASR 1000 Series Route Processor 1(Cisco ASR1000-RP1), the Cisco ASR1000-RP2, supports:

- Memory scalability up to 16 GB DRAM
- 8 GB or 16 GB of synchronous dynamic RAM (SDRAM) in 4 SDRAM slots. A route processor with 8 GB can hold four 8 GB dual in-line memory modules (DIMMs); whereas a route processor with 16 GB can hold four 4-GB DIMMs.
- 80 GB hard disk drive (HDD) for the storage and portability of code storage, boot, configurations, logs.

The Cisco ASR1000-RP2 is supported as a modular component on the Cisco ASR 1004 and Cisco ASR 1006 routers.

The Cisco ASR 1006 Router contains two RP slots to support full hardware redundancy for RP2s within the same router.

For information about the Cisco ASR1000-RP2, including a table that highlights the major differences between it and the Cisco ASR1000-RP1, see the following document:

Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/install/guide/asr1routers/asr1higV8.html

New Shared Port Adapters

Cisco IOS XE Release 2.3.0 introduces support for the following new shared port adapters (SPAs):

ATM SPAs

- 1-Port OC-3 ATM SPA (SPA-1XOC3-ATM-V2)
- 3-Port OC-3 ATM SPA (SPA-3XOC3-ATM-V2)

For information about the SPAs supported on the Cisco ASR 1000 Series Routers, see the following documents:

- *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide* at the following location:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/ASR1000/asr_sip_spa_hw.html

- *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide* at the following location:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ASR1000/ASRspasw.html

New Software Features in Cisco IOS XE Release 2.3.0

This section lists new and changed features in Cisco IOS XE Release 2.3.0. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS XE Release 2.3.0.

- Any Transport Over MPLS (AToM): ATM Cell Relay Over MPLS: VP Mode
- Any Transport over MPLS (AToM): Graceful Restart
- Any Transport Over MPLS (AToM): Layer 2 QoS (Quality of Service)
- Any Transport Over MPLS (AToM): Single Cell Relay - VC Mode (CRoMPLS)
- ATM Conditional debug/show Commands
- ATM MIB Enhancements
- ATM OAM Ping
- ATM OAM Traffic Reduction
- ATM PVC F5 OAM Recovery Traps
- ATM PVC Trap Enhancements for Segment and AIS/RDI Failures

- ATM PVC Trap Support
- ATM SNMP Trap and OAM Enhancements
- ATM VC Class Support
- ATM VP Average Traffic Rate
- AToM Tunnel Selection
- Auto Secure Manageability
- Basic ATM Support of RFC1483
- BGP Support for 4-Byte ASN
- Cell-Based ATM Shaping per PVP
- Consistent and User-Selectable Fail/Open and Fail/Close Operation
- Control Plane Policing—Time Based
- DHCP Client
- DHCP Relay—MPLS VPN Support
- Enhanced ATM VC Configuration and Management
- Explicit Passive Mode CLI Support
- GET VPN Phase 1.2
- Group Encrypted Transport VPN (GET VPN)
- Integrated Session Border Controller
- IPv6 Bidirectional PIM
- IPv6 Multicast: Address Family Support for Multiprotocol BGP
- IPv6 Source Specific Multicast (SSM) Mapping
- ISSU—ATM
- ISSU—AToM ATM Attachment Circuit
- ISSU—MPLS Traffic Engineering (TE)—Path Protection
- L2VPN PW Preferential Forwarding (Active/Standby Status)
- L2VPN PW Redundancy—ATM Attachment Circuits
- LSP Ping for FEC129 (via VCCV)—RFC4379
- MPLS EM—LSP Ping/Trace for LDP & RSVP IPv4 FECs
- MPLS EM—MPLS FRR MIB (IETF draft v01)
- MPLS EM—MPLS Multipath (ECMP) LSP Tree Trace
- MPLS EM—MPLS TE MIB (IETF draft v05)
- MPLS LSP Ping/Traceroute and AToM VCCV
- MPLS Pseudowire Status Signaling
- MPLS Support for Multi-Segment PWs—MPLS OAM/VCCV
- MPLS TE—BFD-Triggered Fast Reroute (FRR)
- MPLS TE—Fast Tunnel Interface Down Detection
- MPLS TE—Node Protection Desired Bit
- MPLS Traffic Engineering Forwarding Adjacency

- MPLS Traffic Engineering—Policy Routing onto MPLS TE Tunnels
- MPLS Traffic Engineering (TE)
- MPLS Traffic Engineering (TE)—Configurable Path Calculation Metric for Tunnels
- MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection
- MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion
- MPLS Traffic Engineering (TE)—LSP Attributes
- MPLS Traffic Engineering (TE)—Path Protection
- MPLS Traffic Engineering (TE)—RSVP Graceful Restart
- MPLS Traffic Engineering (TE)—RSVP Hello State Timer
- MPLS Traffic Engineering (TE): Verbatim Path Support
- MPLS VPN—Explicit Null Label Support with BGP IPv4 Label Session
- NBAR Protocols
- NSF/SSO—AToM ATM Attachment Circuit
- NSF/SSO—MPLS TE and RSVP Graceful Restart
- NSF/SSO—MPLS Traffic Engineering (TE)—Path Protection
- Operation, Administration, and Maintenance (OAM) F4 and F5
- Per-VC Queueing for ATM
- PPP—Max-Payload and IWF PPPoE Tag Support
- PPPoE Agent Remote ID and DSL Line Characteristics Enhancement
- PPPoE Circuit-ID Tag Processing
- PPPoE Relay
- PPPoE—Session Limiting on Inner QinQ VLAN
- Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, FR, and ATM Services
- QoS: Match ATM CLP
- QoS-per-VC QoS Classification for ATM VP Pseudowires
- QoS Priority Percentage CLI Support
- Quality of Service: Policies Aggregation
- RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements
- RSVP Refresh Reduction and Reliable Messaging
- RSVP—Resource Reservation Protocol
- SSO—ATM

Any Transport Over MPLS (AToM): ATM Cell Relay Over MPLS: VP Mode

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_any_transport.html

Any Transport over MPLS (AToM): Graceful Restart

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_atom_grace_rstrt.html

Any Transport Over MPLS (AToM): Layer 2 QoS (Quality of Service)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_any_transport.html

Any Transport Over MPLS (AToM): Single Cell Relay - VC Mode (CRoMPLS)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_any_transport.html

ATM Conditional debug/show Commands

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_con_deb_supp.html

ATM MIB Enhancements

The Cisco AAL5 MIB adds a proprietary extension to the standard ATM MIB (RFC 1695) to provide per-VC statistic counters that are currently displayed in response to the Cisco IOS **show atm vc** command for a specified virtual circuit. This MIB extension allows SNMP network management system applications to query the same variables (SNMP objects) as those that can be gathered from the Cisco IOS command- line interface.

The Cisco AAL5 MIB provides SNMP access to four new statistics counters defined for AAL5 virtual connections: incoming packet counter, outgoing packet counter, incoming octet counter, and outgoing octet counter. The Cisco AAL5 MIB groups these four counters in a table called cAal5VccTable.

The proprietary extension of the Cisco AAL5 MIB supports all the tables and objects defined in the Cisco AAL5 MIB for ATM interfaces acting as endpoints of ATM connections that run Cisco IOS XE Release 2.3 software and later releases.

ATM OAM Ping

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_oam_ping.html

ATM OAM Traffic Reduction

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_oam.html

ATM PVC F5 OAM Recovery Traps

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_cfg_atm.html

ATM PVC Trap Enhancements for Segment and AIS/RDI Failures

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_oam_f5_cnck.html

ATM PVC Trap Support

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_snmp_oam_enh.html

ATM SNMP Trap and OAM Enhancements

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_snmp_oam_enh.html

ATM VC Class Support

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_any_transport.html

ATM VP Average Traffic Rate

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_vp_avg_tfc_rate.html

AToM Tunnel Selection

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_any_transport.html

Auto Secure Manageability

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_autosecure.html

Basic ATM Support of RFC1483

The Basic ATM Support of RFC1483 feature provides the basic functions of asynchronous transfer mode (ATM) and compliance with RFC1483.

Documentation URLs are being updated and will be provided soon.

BGP Support for 4-Byte ASN

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_overview.html

Cell-Based ATM Shaping per PVP

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/qos_atm_vp_support.html

Consistent and User-Selectable Fail/Open and Fail/Close Operation

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_encrypt_trns_vpn.html

Control Plane Policing—Time Based

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/ctrl_plane_policng.html

DHCP Client

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_client.html

DHCP Relay—MPLS VPN Support

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rly_agt.html

Enhanced ATM VC Configuration and Management

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_cfg_atm.html

Explicit Passive Mode CLI Support

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_encrypt_trns_vpn.html

GET VPN Phase 1.2

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_encrypt_trns_vpn.html

Group Encrypted Transport VPN (GET VPN)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_encrypt_trns_vpn.html

Integrated Session Border Controller

Cisco IOS XE Release 2.3.0 introduces support for the following new Integrated Session Border Controller (SBC) features:

- In-Service Provisioning of H.248 Controllers
- RTCP Policing (with the additional new functionality of RTCP maximum burst size (mbs) policing equal to 5% of RTP mbs)

For information about these SBC features, see the following document:

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbc/2_xe/sbc_2_xe_book.html

IPv6 Bidirectional PIM

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html

IPv6 Multicast: Address Family Support for Multiprotocol BGP

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html

IPv6 Source Specific Multicast (SSM) Mapping

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html

ISSU—ATM

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ha/configuration/guide/ha-inserv_updg_xe.html

ISSU—AToM ATM Attachment Circuit

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_trnsprt_mlps_atom.html

ISSU—MPLS Traffic Engineering (TE)—Path Protection

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_path_prot.html

L2VPN PW Preferential Forwarding (Active/Standby Status)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/l2vpn_pw_preferential_forwarding.html

L2VPN PW Redundancy—ATM Attachment Circuits

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_l2vpn_pw_red_ps9587_TSD_Products_Configuration_Guide_Chapter.html

LSP Ping for FEC129 (via VCCV)—RFC4379

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ldp_te_lsp_vccv.html

MPLS EM—LSP Ping/Trace for LDP & RSVP IPv4 FECs

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ldp_te_lsp_vccv.html

MPLS EM—MPLS FRR MIB (IETF draft v01)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_fast_rr_mib.html

MPLS EM—MPLS Multipath (ECMP) LSP Tree Trace

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_em_multipath_tree.html

MPLS EM—MPLS TE MIB (IETF draft v05)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_mib.html

MPLS LSP Ping/Traceroute and AToM VCCV

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ldp_te_lsp_vccv.html

MPLS Pseudowire Status Signaling

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_pw_status.html

MPLS Support for Multi-Segment PWs—MPLS OAM/VCCV

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/multisegmentpseudowires.html

MPLS TE—BFD-Triggered Fast Reroute (FRR)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_bfd_frr.html

MPLS TE—Fast Tunnel Interface Down Detection

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_link_node_prot.html

MPLS TE—Node Protection Desired Bit

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_link_node_prot.html

MPLS Traffic Engineering Forwarding Adjacency

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_fwd_adjacency.html

MPLS Traffic Engineering—Policy Routing onto MPLS TE Tunnels

Cisco IOS XE Release 2.3.0 supports mapping packets to MPLS Traffic Engineering tunnels.

For more information, see the **set interface** command in the *Cisco IOS IP Routing Protocols Command Reference* at the following URL:

http://www.cisco.com/en/US/docs/ios/iproute/command/reference/irp_pi2.html

MPLS Traffic Engineering (TE)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_enhance.html

MPLS Traffic Engineering (TE)—Configurable Path Calculation Metric for Tunnels

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_cfg_path_calc.html

MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_frr_node_prot.html

MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_expl_address.html

MPLS Traffic Engineering (TE)—LSP Attributes

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_lsp_attr.html

MPLS Traffic Engineering (TE)—Path Protection

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_path_prot.html

MPLS Traffic Engineering (TE)—RSVP Graceful Restart

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_rsvp_graceful.html

MPLS Traffic Engineering (TE)—RSVP Hello State Timer

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_rsvp_hello.html

MPLS Traffic Engineering (TE): Verbatim Path Support

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_verbatim_path.html

MPLS VPN—Explicit Null Label Support with BGP IPv4 Label Session

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ce_vpn_explicit.html

NBAR Protocols

For information about this feature, see the following document, which also includes a table listing the NBAR protocol support per Cisco IOS XE release:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/clsfy_traffic_nbar_xe.html

NSF/SSO—AToM ATM Attachment Circuit

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_trnsprt_mlps_atom.html

NSF/SSO—MPLS TE and RSVP Graceful Restart

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_te_rsvp_graceful_xe.html

NSF/SSO—MPLS Traffic Engineering (TE)—Path Protection

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_path_prot.html

Operation, Administration, and Maintenance (OAM) F4 and F5

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_oam_f5_cnck.html

Per-VC Queueing for ATM

The Per-VC Queueing for ATM feature on the Cisco ASR 1000 Series Routers supports two sets of queues on a virtual circuit (VC):

- Queues on a Shared Port Adapter (SPA) that uses segmentation and reassembly (SAR)
- Queues on a Cisco QuantumFlow Processor (QFP)

Configurable SAR queues are not supported on Cisco ASR 1000 Series Routers. SAR allocates two queues per VC, one for high-priority traffic and another for low-priority traffic.

ATM QoS queueing operations on a QFP are carried out using the Modular QoS CLI (MCQ). The **tx_limit** command is used to change queue size on the QFP.

PPP—Max-Payload and IWF PPPoE Tag Support

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_ppp_mx_payld_xe.html

PPPoE Agent Remote ID and DSL Line Characteristics Enhancement

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_rmtid_dsl_xe.html

PPPoE Circuit-ID Tag Processing

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_cir_id_tag_pr_xe.html

PPPoE Relay

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_relaydis_ssf_xe.html

PPPoE—Session Limiting on Inner QinQ VLAN

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/bbdsl/configuration/guide/bba_qinq_vlan_limt_xe.html

Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, FR, and ATM Services

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_edge2edge_mibs.html

QoS: Match ATM CLP

For information about this feature, see the following document:

http://cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/clsfy_netwk_traffic_xe_ps9587_TSD_Products_Configuration_Guide_Chapter.html

QoS-per-VC QoS Classification for ATM VP Pseudowires

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/qos_atm_vp_support.html

QoS Priority Percentage CLI Support

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/llq_with_pps_xe.html

Quality of Service: Policies Aggregation

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/qos_policies_agg_xe.html

RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_rad_a66_enhcmts.html

RSVP Refresh Reduction and Reliable Messaging

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/rsvp_messaging.html

RSVP—Resource Reservation Protocol

The RSVP—Resource Reservation Protocol feature is supported for Multiprotocol Label Switching (MPLS) traffic engineering (TE) based on RFC 2205, *Resource ReSerVation Protocol (RSVP - Version 1 Functional Specification*, http://www.apps.ietf.org/rfc/rfc2205.html. To enable RSVP, see the **ip rsvp bandwidth** command in the *Cisco IOS Quality of Service Solutions Command Reference*.

SSO—ATM

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ha/configuration/guide/ha-stfl_swovr_xe.html

New Hardware Features in Cisco IOS XE Release 2.2.3

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.2.3.

New Software Features in Cisco IOS XE Release 2.2.3

This section lists new and changed features in Cisco IOS XE Release 2.2.3. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS XE Release 2.2.3.

- MPLS VPN Carrier Supporting Carrier Using LDP and an IGP
- MPLS VPN Carrier Supporting Carrier with BGP
- MPLS VPN—eBGP Multipath Support for CSC and InterAS MPLS VPNs
- MPLS VPN—Load Balancing Support for Inter-AS and CSC VPNs

MPLS VPN Carrier Supporting Carrier Using LDP and an IGP

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_carrier_ldp_igp.html

MPLS VPN Carrier Supporting Carrier with BGP

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_carrier_bgp.html

MPLS VPN—eBGP Multipath Support for CSC and InterAS MPLS VPNs

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_load_share_vpn.html

MPLS VPN—Load Balancing Support for Inter-AS and CSC VPNs

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_load_share_vpn.html

New Hardware Features in Cisco IOS XE Release 2.2.2

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.2.2.

New Software Features in Cisco IOS XE Release 2.2.2

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.2.2.

New Hardware Features in Cisco IOS XE Release 2.2.1

The following new hardware features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.2.1:

- New Cisco ASR 1000 Embedded Services Processors
- New Shared Port Adapters

New Cisco ASR 1000 Embedded Services Processors

Cisco IOS XE Release 2.2.1 introduces support for the following new Embedded Services Processors (ESPs):

Cisco ASR 1000 Embedded Services Processor 10G Non Crypto Capable

The Cisco ASR 1000 Embedded Services Processor 10G Non Crypto Capable (Cisco ASR1000-ESP10-N) is a non-crypto capable version of the encryption-enabled 10-Gbps Cisco ASR 1000 Series ESP (Cisco ASR1000-ESP10).

The Cisco ASR 1000 Embedded Services Processor 10G Non Crypto Capable provides a Cisco ASR 1000 solution for customers who are under export restrictions and not qualified to implement products that support strong encryption services. The Cisco ASR 1000 Embedded Services Processor 10G Non Crypto Capable feature support is the same as the 10-Gbps Cisco ASR 1000 Series ESP except that IPSec and other data-plane cryptographic features are not supported.

The Cisco ASR 1000 Embedded Services Processor 10G Non Crypto Capable is supported on all Cisco ASR 1000 Series chassis but should only be used with following consolidated packages that do not contain cryptographic (K9) software:

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

Note The Cisco ASR 1000 Series RP1 IP BASE W/O CRYPTO, Cisco ASR 1000 Series RP1 ADVANCED IP SERVICES W/O CRYPTO, and Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES W/O CRYPTO consolidated packages do not require export qualification and can also run on the encryption-enabled 10-Gbps Cisco ASR 1000 Series ESP. The K9-based consolidated packages (Cisco ASR 1000 Series RP1 IP BASE, Cisco ASR 1000 Series RP1 ADVANCED IP SERVICES and Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES) will never be supported on the Cisco ASR 1000 Embedded Services Processor 10G Non Crypto Capable hardware.

Note The Cisco ASR 1000 Embedded Services Processor 10G Non Crypto Capable should never be inserted into a chassis using K9 software or the router may reload.

Note The Cisco ASR 1000 Embedded Services Processor 10G Non Crypto Capable and 10-Gbps Cisco ASR 1000 Series ESP should not be mixed in a hardware-redundant chassis.

For information about the Cisco ASR 1000 Embedded Services Processor 10G Non Crypto Capable, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/install/guide/asr1routers/asr1higV8.html

Cisco ASR 1000 Embedded Services Processor 10G Non Crypto Capable New Feature at the following location:

http://www.cisco.com/en/US/partner/docs/routers/asr1000/feature/guides/ASR_depop.html

20-Gbps Cisco ASR 1000 Series ESP

The 20-Gbps Cisco ASR 1000 Series ESP (Cisco ASR1000-ESP20) supports 20-Gbps bandwidth and is supported on the Cisco ASR 1004 and Cisco ASR 1006 chassis. It can optionally be deployed in customer networks that require 1+1 redundancy on Cisco ASR 1006 Routers. Performance highlights of the 20-Gbps ESP include hardware-assisted policing, encryption capability of 8 Gbps, 16 Mpps forwarding, 256MB of packet memory, 1GB (bytes) of resource memory performance, and special jitter- and latency-minimizing multicast packet replication.

For information about the 20-Gbps Cisco ASR 1000 Series ESP, see the following document:

Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/install/guide/asr1routers/asr1higV8.html

New Shared Port Adapters

Cisco IOS XE Release 2.2.1 introduces support for the following new shared port adapters (SPAs):

Channelized SPA

- 1-Port CHOC-3/CHSTM-1 SPA (SPA-1xCHSTM1/OC3)

POS SPAs

- 2-Port OC-48 POS/RPR SPA with SFP Optics (SPA-2XOC48POS/RPR)
- 4-Port OC-48 POS/RPR SPA with SFP Optics (SPA-4XOC48POS/RPR)

For information about the SPAs supported on the Cisco ASR 1000 Series Routers, see the following documents:

- *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide* at the following location:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/ASR1000/asr_sip_spa_hw.html

- *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide* at the following location:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ASR1000/ASRspasw.html

New Software Features in Cisco IOS XE Release 2.2.1

This section lists new and changed features in Cisco IOS XE Release 2.2.1. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS XE Release 2.2.1.

- AAA Broadcast Accounting
- Bidirectional PIM
- Cisco Firewall and WAAS Inter-Op
- Class-Based Marking
- Class Based Weighted Fair Queuing (CBWFQ)
- Control Plane Policing (CoPP)

- Diffie-Hellman Group Support in IPSec
- FPM—Flexible Packet Matching
- GPI (Granular Protocol Inspection) Phase-1
- GRE Tunnel IP Source and Destination VRF Membership
- Integrated Session Border Controller
  - Full Support for Wildcard Response
  - H.248 Protocol—Acknowledgment Support for Three-Way Handshake
  - H.248 ServiceChange Handoff
  - Improved Media Timeout Detection
  - Interim Authentication Header Full Support
  - IPSec Pinhole Support—Twice NAT for IPv4 and No NAT for IPv6
- IP SLAs—LSP Health Monitor
- IP SLAs—LSP Health Monitor with LSP Discovery
- IP SLAs—MPLS VPN Awareness
- IPv6 QoS: MQC Packet Classification
- IPv6 Routing—EIGRP Support
- ISG: Accounting: Per Session, Service and Flow
- ISG: Accounting: Postpaid
- ISG: Accounting: Tariff Switching
- ISG: Authentication: DHCP Option 82 Line ID - AAA Authorization Support
- ISG:Flow Control: Flow Redirect (L4, Captive Portal)
- ISG: Flow Control: QoS Control: Dynamic Rate Limiting (QU;QD)
- ISG: Flow Control: QoS Control: MQC Support for IP Sessions
- ISG: Instrumentation: Advanced Conditional Debugging
- ISG: Instrumentation: Session and Flow Monitoring (Local and External)
- ISG: Network Interface: IP Routed, VRF Aware MPLS
- ISG: Network Interface: Tunneled (L2TP)
- ISG: Policy Control: Cisco Policy Language
- ISG: Policy Control: DHCP Proxy
- ISG: Policy Control: ISG-SCE Control Bus
- ISG: Policy Control: Multidimensional Identity per Session
- ISG: Policy Control: Policy: Domain Based (Auto-Domain, Proxy)
- ISG: Policy Control: Policy Server: CoA ASCII Command Code Support
- ISG: Policy Control: Policy Server: CoA (QoS, L4 Redirect, User ACL, TimeOut)
- ISG: Policy Control: Policy Server: SSG-SESM Protocol
- ISG: Policy Control: Policy: Triggers (Time, Volume, Duration)
- ISG: Policy Control: RADIUS Proxy Enhancement
- ISG: Policy Control: Service Profiles

- ISG: Policy Control: User Profiles
- ISG: Session: Auth: Single Sign On
- ISG: Session: Authentication (MAC, IP, EAP)
- ISG: Session: Creation: IP Session: Protocol Event (DHCP, RADIUS)
- ISG: Session: Creation: IP Session: Subnet and Source IP: L2
- ISG: Session: Creation: IP Session: Subnet and Source IP: L3
- ISG: Session: Creation: P2P Session (PPPoE, PPPoXoX)
- ISG: Session: LifeCycle: Idle Timeout
- ISG: Session: LifeCycle: POD
- ISG: Session: Multi-Service Creation and Flow Control
- ISG: Session: Protection and Resiliency: Keepalive—ARP, ICMP
- ISG: Session: VRF Transfer
- L2TP AAA Accounting Include NAS-PORT (VPI/VCI)
- L2TP HA Session SSO/ISSU on LAC/LNS
- L3 MPLS VPN Over GRE
- MPLS LDP— VRF Aware Static Labels
- MPLS VPN—Per VRF Label
- MPLS VPN: VRF Selection Using Policy Based Routing
- Multihop VPDN
- Multi-VRF Selection Using Policy Based Routing (PBR)
- NAT—Routemaps Outside-to-Inside Support
- Packet Classification Based on Layer3 Packet-Length
- PBR Support for Multiple Tracking Options
- Per Subscriber Firewall on LNS
- Policy-Based Routing (PBR)
- Policy-Based Routing (PBR) Default Next-Hop Route
- Policy Based Routing: Recursive Next Hop
- Policy Routing Infrastructure
- PPPoE—QinQ Support
- QoS—Hierarchical Queuing for Ethernet DSLAMs
- RADIUS Route Download
- Remote Access to MPLS-VPNs
- SGI Interface
- VRF Aware System Message Logging (Syslog)
- VRF-Aware VPDN Tunnels
- WCCP L2 Return
- WCCP Layer 2 Redirection / Forwarding
- WCCP Mask Assignment

- WCCP Redirection on Inbound Interfaces
- WCCP Version 2

AAA Broadcast Accounting

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_accountg.html

Bidirectional PIM

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_basic_cfg.html

Cisco Firewall and WAAS Inter-Op

The Cisco Firewall and WAAS Interoperability feature enables a router configured with a firewall to successfully communicate with a cache engine, such as a Wide Area Application Acceleration (WAAS) device that is using the Web Cache Communication Protocol (WCCP).

WAAS optimizes remote access to applications.When the cache engine is a WAAS device, it can optimize TCP flow by modifying TCP headers. During the TCP three-way handshake, the WAAS device can add an extra TCP option in the header to indicate that the flow will be optimized. When the TCP session is established, the WAAS device can modify the sequence and acknowledge number in the TCP header to optimize the data flow.

When a Cisco firewall is configured on the router, the packets have to be inspected by the firewall. Depending on the deployment scenario, the firewall inspects packets as follows:

- For client-to-server packets, the firewall inspects packets in the redirect path and ignores packets in the return path.
- For server-to-client packets, the firewall inspects packets in the return path and ignores packets in the redirect path.
- If the firewall encounters a TCP SYN packet with the 0x21 option, the firewall knows that this packet is already a WAAS flow. The firewall will adjust the Layer 4 state to reflect the 2-GB jump in sequence and acknowledge numbers. No Layer 7 inspection will be applied to the flow.
- Although the firewall will ignore the same packets in either the redirect or the return path, the firewall must still perform a session lookup to get the information about the direction of the packet (from client to server or server to client).

This feature has the following restrictions:

- 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.

Class-Based Marking

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/mrkg_netwk_traffic.html

Class Based Weighted Fair Queuing (CBWFQ)

CBWFQ extends the standard weighted fair queueing (WFQ) functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria such as protocols, access control lists (ACLs), and input interfaces.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_wfq.html

Control Plane Policing (CoPP)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/ctrl_plane_policng.html

Diffie-Hellman Group Support in IPSec

The Diffie-Hellman Group Support in IPSec feature adds support for Diffie-Hellman groups 14, 15, and 16.

For more information, see the **group (IKE policy)** and **set pfs** commands in the following document:

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html

FPM—Flexible Packet Matching

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_flex_pack_match.html

GPI (Granular Protocol Inspection) Phase-1

The feature GPI (Granular Protocol Inspection) Phase-1 allows for support for the following 10 protocols:

GTP (Granular Protocol Inspection) - FTP (File Transfer Protocol)

GTP - H.323

GTP - ICMP

GTP - RTSP (Real Time Streaming Protocol)

GTP -SIP (Session Initiation Protocol)

GTP - Skinny Client Control Protocol

GTP - TCP

GTP - TFTP (Trivial File Transfer Protocol)

GTP - UDP

GRE Tunnel IP Source and Destination VRF Membership

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/interface/configuration/guide/ir_impl_tun.html

Integrated Session Border Controller

Cisco IOS XE Release 2.2.1 introduces support for the following new Integrated Session Border Controller (SBC) features:

- Full Support for Wildcard Response
- H.248 Protocol—Acknowledgment Support for Three-Way Handshake
- H.248 ServiceChange Handoff
- Improved Media Timeout Detection
- Interim Authentication Header Full Support
- IPSec Pinhole Support—Twice NAT for IPv4 and No NAT for IPv6

Full Support for Wildcard Response

Previously Session Border Controller (SBC) supported H.248 wildcard operations that were restricted to W-Modify or W-Subtract requests, which yielded summary wildcard responses. This feature introduces support for a complete wildcard response. A wildcard H.248 Subtract or Modify operation now returns a complete response with per-termination statistics.

H.248 Protocol—Acknowledgment Support for Three-Way Handshake

The data border element (DBE) supports a three-way handshake for H.248 messages. The DBE supports sending of an acknowledgement for a three-way handshake after receiving the transaction response from the media gateway controller (MGC), as described in Annex D.1.2 and Annex D.1.2.2 of H.248.1 v3 Gateway Control Protocol.

H.248 ServiceChange Handoff

The ServiceChange Handoff functionality on Integrated Session Border Controller conforms to section 7.2.8, ServiceChange, and section 7.2.8.1.1, ServiceChangeMethod, of the H.248.1 v3 Gateway Control Protocol. The ServiceChange Handoff functionality allows a media gateway controller (MGC) to hand over control of a media gateway (MG) to another MGC. The MGC sends a ServiceChange message to the MG that it is currently associated with to request that the MG terminate that association and the MG form a new association with an MGC identified in the ServiceChange message.

Improved Media Timeout Detection

In the previous media timeout functionality on the data border element (DBE), if no SBC packets have been seen by the configured number of seconds since the call has been established, then the DBE generates a media timeout alert to the SBE. The Improved Media Timeout Detection feature delays reporting of the media timeout event by instructing the DBE to wait until it has received the first packet since the call has been established. Only then does the media timeout timer start counting the number of seconds for which it has not seen an SBC packet. At the end of the count, the DBE generates an alert to the SBE.

Interim Authentication Header Full Support

Integrated SBC offers full support of Interim Authentication Header (IAH) that conforms to section 10.2, Interim AH Scheme, of the H.248.1 v3 Gateway Control Protocol. An IAH is part of every H.248 message generated by the data border element (DBE) to the media gateway controller (MGC). Information in the IAH is used to authenticate and check the integrity of packets, thus ensuring packet security. The DBE generates an IAH for outgoing H.248 messages and can verify the Authentication Header for incoming H.248 messages. The IAH scheme inserts the IAH within the H.248.1 protocol header.

IPSec Pinhole Support—Twice NAT for IPv4 and No NAT for IPv6

The IPSec Pinhole Support—Twice NAT for IPv4 and No NAT for IPv6 feature adds support for voice calls over IPSec tunnels and adds support for IPSec address-only pinholes. This support enables the DBE to forward IPSec packets when the port cannot be determined because the port is within the encrypted portion of the frame. Thus, IPSec support handles the IPSec requirement that does not allow use of port numbers for session lookup or translation. Currently single IPSec pinholes are supported, whereby both IKE and the encrypted IPSec traffic passes through the same pinhole.

For information about these SBC features, see the following document:

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbc/2_xe/sbc_2_xe_book.html

IP SLAs—LSP Health Monitor

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_lsp_mon_autodisc.html

IP SLAs—LSP Health Monitor with LSP Discovery

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_lsp_mon_autodisc.html

IP SLAs—MPLS VPN Awareness

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_overview.html

IPv6 QoS: MQC Packet Classification

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-qos.html

IPv6 Routing—EIGRP Support

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-eigrp.html

ISG: Accounting: Per Session, Service and Flow

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Accounting: Postpaid

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Accounting: Tariff Switching

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Authentication: DHCP Option 82 Line ID - AAA Authorization Support

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG:Flow Control: Flow Redirect (L4, Captive Portal)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Flow Control: QoS Control: Dynamic Rate Limiting (QU;QD)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Flow Control: QoS Control: MQC Support for IP Sessions

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Instrumentation: Advanced Conditional Debugging

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Instrumentation: Session and Flow Monitoring (Local and External)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Network Interface: IP Routed, VRF Aware MPLS

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Network Interface: Tunneled (L2TP)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Policy Control: Cisco Policy Language

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Policy Control: DHCP Proxy

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Policy Control: ISG-SCE Control Bus

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Policy Control: Multidimensional Identity per Session

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Policy Control: Policy: Domain Based (Auto-Domain, Proxy)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Policy Control: Policy Server: CoA ASCII Command Code Support

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Policy Control: Policy Server: CoA (QoS, L4 Redirect, User ACL, TimeOut)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Policy Control: Policy Server: SSG-SESM Protocol

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Policy Control: Policy: Triggers (Time, Volume, Duration)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Policy Control: RADIUS Proxy Enhancement

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Policy Control: Service Profiles

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Policy Control: User Profiles

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Session: Auth: Single Sign On

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Session: Authentication (MAC, IP, EAP)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Session: Creation: IP Session: Protocol Event (DHCP, RADIUS)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Session: Creation: IP Session: Subnet and Source IP: L2

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Session: Creation: IP Session: Subnet and Source IP: L3

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Session: Creation: P2P Session (PPPoE, PPPoXoX)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Session: LifeCycle: Idle Timeout

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Session: LifeCycle: POD

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Session: Multi-Service Creation and Flow Control

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Session: Protection and Resiliency: Keepalive—ARP, ICMP

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

ISG: Session: VRF Transfer

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

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

The L2TP AAA Accounting Include NAS-PORT (VPI/VCI) feature allows an L2TP Network Server (LNS) to send the NAS Port-ID (attribute 5), as part of the accounting record to the RADIUS authentication, authorization, and accounting (AAA) server.

Limitations and Restrictions

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.

L2TP HA Session SSO/ISSU on LAC/LNS

The L2TP HA Session SSO/ISSU on a LAC/LNS feature provides a generic Stateful Switchover/In Service Software Upgrade (SSO/ISSU) mechanism for Layer 2 Tunneling Protocol (L2TP) on a Layer 2 Access Concentrator (LAC) and a Layer 2 Network Server (LNS). This feature preserves all fully-established Point-to-Point Protocol (PPP) and L2TP sessions (including Multihop) during an SSO switchover, or an ISSU upgrade or downgrade.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/vpdn/configuration/xe-3s/vpd-cfg-l2tp-ha-session-sso-issu-lac-lns.html

L3 MPLS VPN Over GRE

L3 MPLS VPN over GRE provides a mechanism for tunneling Multi Protocol Label Switching (MPLS) packets over a non-MPLS network.

The L3 MPLS VPN over GRE feature utilizes MPLS over Generic Routing Encapsulation (MPLSoGRE) to encapsulate MPLS packets inside IP tunnels; thus creating a virtual point-to-point link across non-MPLS networks. This allows users of primarily MPLS networks to continue to use existing non-MPLS legacy networks until migration to MPLS is possible.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_gre.html

MPLS LDP— VRF Aware Static Labels

The MPLS LDP-VRF-Aware Static Labels document explains how to configure the MPLS LDP-VRF-Aware Static Labels feature and Multiprotocol Label Switching (MPLS) static labels.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vrf_aware_static.html

MPLS VPN—Per VRF Label

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_per_vrf_lbl.html

MPLS VPN: VRF Selection Using Policy Based Routing

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_vrf_select_rt.html

Multihop VPDN

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/vpdn/configuration/guide/config_multihop_vpdn_xe.html

Multi-VRF Selection Using Policy Based Routing (PBR)

The Multi-VRF Selection Using Policy-Based Routing feature allows a specified interface on a provider edge (PE) router to route packets to Virtual Private Networks (VPNs) based on packet length or match criteria defined in an IP access list.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_mltvrf_slct_pbr.html

NAT—Routemaps Outside-to-Inside Support

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/ipaddr/configuration/guide/iadnat_addr_consv_xe.html

Packet Classification Based on Layer3 Packet-Length

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/class_l3_pkt_length.html

PBR Support for Multiple Tracking Options

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_prb_mult_track.html

Per Subscriber Firewall on LNS

The Per-Subscriber Firewall on LNS feature enables the zone-based policy firewall configuration model to be implemented on the Cisco ASR 1000 Series Router. Zone-based policy firewall is a unidirectional firewall policy between groups of interfaces known as zones. (Previously, Cisco firewalls were configured as an inspect rule only on interfaces. Traffic entering or leaving the configured interface was inspected based on the direction that the inspect rule was applied.) Now, interfaces are assigned to zones, and inspection policies are applied to traffic moving between the zones. Interzone policies offer considerable flexibility and granularity, so different inspection policies can be applied to multiple host groups connected to the same router interface.

In addition to the zone-based policy firewall model, the Per-Subscriber Firewall on LNS feature introduces the following additional functionality for the Cisco ASR 1000 Series Router:

- Dynamic zone assignment for virtual access interfaces

  Subscribers can be assigned to a zone in one of two ways:

  - Using the configuration on the virtual-template interface, which can be useful when placing subscribers in a default zone.
  - Using the RADIUS vendor-specific attribute (VSA), which enables zone assignment to be determined when the session is authorized.

- PPP session-level granularity for zone-based policy firewall

  Stateful inspection and application monitoring occur at the PPP session, enabling the full suite of firewall and broadband features to be applied per subscriber, simultaneously. That is, extra routers or service blades are not required to support the firewall functionality. The firewall functionality is applied by the packet processor engine (PPE) in the forwarding path for broadband traffic.

- Per-subscriber drop log messages

  Service providers can track drops on a per-subscriber basis by including the subscriber's username in the drop log messages. These drop log messages can also be sent to an off-box server for additional processing.

- Zone pairs with matching source and destination zones

  Service providers can customize the firewall policy for traffic between subscribers in the same zone. Customization is useful for overriding the default behavior, which is the passage of all traffic within the same zone.

For more information on zone-based policy firewalls, see the following documents:

- *Zone-Based Policy Firewall*

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_zone_polcy_firew.html

- *Zone-based Policy Firewall Design and Application Guide*

  http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml

Policy-Based Routing (PBR)

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_ip_prot_indep.html

Note Cisco IOS XE Release 2 only supports PBR on IPv4; Cisco IOS Release 2 does not support IPv6 PBR.

Policy-Based Routing (PBR) Default Next-Hop Route

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_ip_prot_indep.html

Policy Based Routing: Recursive Next Hop

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute/configuration/guide/irp_prb_rec_next_hop_xe.html

Policy Routing Infrastructure

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_ip_prot_indep.html

PPPoE—QinQ Support

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/bbdsl/configuration/guide/bba_pppoe_qinq.html

QoS—Hierarchical Queuing for Ethernet DSLAMs

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/hier_que_eth_dslams.html

RADIUS Route Download

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_rad_route_dwnld.html

Remote Access to MPLS-VPNs

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ra_mpls_vpns.html

SGI Interface

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/2_xe/isg_2_xe_book.html

VRF Aware System Message Logging (Syslog)

The VRF Aware System Message Logging (Syslog) feature allows a router to send system logging (syslog) messages to a syslog server host connected through a Virtual Private Network (VPN) routing and forwarding (VRF) interface.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vrf_aware_loggng.html

VRF-Aware VPDN Tunnels

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/vpdn/configuration/guide/additional_vpdn_feat_xe.html

WCCP L2 Return

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_wccp.html

WCCP Layer 2 Redirection / Forwarding

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_wccp.html

WCCP Mask Assignment

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_wccp.html

WCCP Redirection on Inbound Interfaces

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_wccp.html

WCCP Version 2

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_wccp.html

New Hardware Features in Cisco IOS XE Release 2.1.2

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.1.2.

New Software Features in Cisco IOS XE Release 2.1.2

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.1.2.

New Hardware Features in Cisco IOS XE Release 2.1.1

There are no new hardware features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.1.1.

New Software Features in Cisco IOS XE Release 2.1.1

There are no new software features supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.1.1.

New Hardware Features in Cisco IOS XE Release 2.1.0

The following new hardware features are supported by the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.1.0:

- Cisco ASR 1002 Router
- Cisco ASR 1004 Router
- Cisco ASR 1006 Router
- Cisco ASR 1000 Embedded Services Processors
- Cisco ASR 1000 Route Processor 1
- Cisco ASR 1000 SPA Interface Processor
- Shared Port Adapters
- 1GB USB Flash Token for Cisco ASR 1000 Series

Cisco ASR 1002 Router

The Cisco ASR 1002 Router (3-SPA, 2-RU chassis) comes with an integrated Route Processor (RP), an integrated SPA Interface Processor (SIP), four built-in Gigabit Ethernet ports, and is configurable with either the 5 Gbps or 10 Gbps Embedded Services Processor (ESP). The Cisco ASR 1002 Router supports the following components:

- One Cisco ASR 1000 Series Embedded Services Processor (ESP). Either the 5-Gbps Cisco ASR 1000 Series ESP (Cisco ASR1000-ESP5) or the 10-Gbps Cisco ASR 1000 Series ESP (Cisco ASR1000-ESP10).
- One Cisco ASR 1000 Series Route Processor 1 (Cisco ASR1000-RP1) with 4-GB DRAM (memory is not factory- or field-upgradeable) integrated in the chassis
- Four built-in Gigabit Ethernet ports
- One Cisco ASR 1000 SPA Interface Processor 10 (Cisco ASR1000-SIP10) integrated in the chassis
- Up to three fixed SPAs integrated in the chassis
- Dual (redundant) power supplies, option of either AC or DC power supply

Running on Cisco IOS XE Software, the Cisco ASR 1002 Router supports software redundancy, Cisco high-availability features, Nonstop Forwarding (NSF), and In Service Software Upgrades (ISSUs) without redundant hardware.

For information about the Cisco ASR 1002 Router, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/install/guide/asr1routers/asr1higV8.html

Cisco ASR 1002 Quick Start Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/quick/start/guide/asr1_qs2.html

Cisco ASR 1004 Router

The Cisco ASR 1004 Router (8-SPA, 4-RU chassis) comes with one Route Processor (RP) slot, one Embedded Services Processor (ESP) slot, two SPA Interface Processor (SIP) slots, and provides 10 Gbps throughput support. The Cisco ASR 1004 Router supports the following components:

- One Cisco ASR 1000 Series Embedded Services Processor (Cisco ASR1000-ESP10)
- One Cisco ASR 1000 Series Route Processor 1 (Cisco ASR1000-RP1)
- Up to two Cisco ASR 1000 Series SPA Interface Processors (Cisco ASR1000-SIP10s)
- Up to eight SPAs
- Dual (redundant) power supplies, option of either AC or DC power supply

Running on Cisco IOS XE Software, the Cisco ASR 1004 Router supports software redundancy, Cisco high-availability features, NSF, and ISSUs without redundant hardware.

For information about the Cisco ASR 1004 Router, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/install/guide/asr1routers/asr1higV8.html

*Cisco ASR 1004 Quick Start Guide*at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/quick/start/guide/asr1_qs4.html

Cisco ASR 1006 Router

The Cisco ASR 1006 Router (12-SPA, 6-RU chassis) provides the option of hardware-redundant Route Processor (RP) and Embedded Services Processor (ESP) support. Its features include two ESP slots, two RP slots, three SIP slots, and 10 Gbps throughput support. The Cisco ASR 1006 Router supports the following components:

- Dual Cisco ASR 1000 Series Embedded Services Processors (Cisco ASR1000-ESP10s)
- Dual Cisco ASR 1000 Series Route Processor 1s (Cisco ASR1000-RP1s)
- Up to three Cisco ASR 1000 Series SPA Interface Processors (Cisco ASR1000-SIP10s)
- Up to twelve SPAs
- Dual (redundant) power supplies, option of either AC or DC power supply

Note When multiple ESPs, RPs, and SIPs are used, the amount of memory should be equal for like components. (The amount of memory in both ESPs should be equal, the amount of memory in both RPs should be equal, and the amount of memory in each SIP should be equal.) Earlier releases may have a few field replaceable units (FRUs) that support different amounts of memory.

Running on Cisco IOS XE Software, the Cisco ASR 1006 Router supports hardware redundancy, NSF, ISSUs, and future Route-Processor service upgrades.

Note Software redundancy is not supported on the Cisco ASR 1006 Router.

For information about the Cisco ASR 1006 Router, see the following documents:

Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/install/guide/asr1routers/asr1higV8.html

Cisco ASR 1006 Quick Start Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/quick/start/guide/asr1_qs6.html

Cisco ASR 1000 Embedded Services Processors

The Cisco ASR 1000 Series Embedded Services Processors (ESPs) provide the centralized forwarding-engine options for the Cisco ASR 1000 Series Routers. Based on the first generation of the hardware and software architecture known as the Cisco QuantumFlow Processor, the Cisco ASR 1000 Series ESPs are responsible for the data-plane processing tasks, and all network traffic flows through them. The modules perform all baseline packet routing operations, including MAC classification, Layer 2 and Layer 3 forwarding, Quality of Service (QoS) classification, policing and shaping, security access control lists (ACLs), virtual private networks (VPNs), load balancing, and NetFlow. They are also responsible for features such as firewalls, intrusion prevention, Network Based Application Recognition (NBAR), and Network Address Translation (NAT).

The Cisco ASR 1000 Series Routers support two ESPs:

- 5-Gbps Cisco ASR 1000 Series ESP (Cisco ASR1000-ESP5), which is only supported on the Cisco ASR 1002 chassis
- 10-Gbps Cisco ASR 1000 Series ESP (Cisco ASR1000-ESP10), which is supported on all Cisco ASR 1000 Series chassis

5-Gbps Cisco ASR 1000 Series ESP

The 5-Gbps Cisco ASR 1000 Series ESP (Cisco ASR1000-ESP5) supports 5-Gbps bandwidth, an encryption capability of 1 Gbps, and is supported exclusively on the Cisco ASR 1002 chassis.

10-Gbps Cisco ASR 1000 Series ESP

The 10-Gbps Cisco ASR 1000 Series ESP (Cisco ASR1000-ESP10) supports 10-Gbps bandwidth, is supported on all Cisco ASR 1000 Series chassis, and can optionally be deployed in customer networks that require 1+1 redundancy on Cisco ASR 1006 Routers. Performance highlights of the 10-Gbps ESP include hardware-assisted policing, encryption capability of 3 Gbps, and special jitter- and latency-minimizing multicast packet replication.

For information about the 5-Gbps Cisco ASR 1000 Series ESP and the 10-Gbps Cisco ASR 1000 Series ESP, see the following document:

Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/install/guide/asr1routers/asr1higV8.html

Cisco ASR 1000 Route Processor 1

The Cisco ASR 1000 Series Route Processor 1 (Cisco ASR1000-RP1) is the main control plane processor in the chassis and is responsible for:

- All control processor communication (such as running the operating system, managing control traffic, storing files, system logging, and most management-type tasks).
- Processing locally destined control-plane packets and RP-switched packets.
- Central network clocking.
- Certain control plane functions related to PPPoE and Session Border Controller (SBC) functions. (These functions are the single largest source of RP overhead.)
- Cisco ASR 1000 Series field replaceable unit (FRU) online insertion and removal (OIR).
- Selection of the active Cisco ASR1000-RP1 and Cisco ASR 1000 Series Embedded Services Processor, and notification of the SIP of these events.

On the Cisco ASR 1002 Router, the Cisco ASR1000-RP1 is integrated in the chassis and comes with 4-GB DRAM (memory is neither factory- nor field-upgradeable).

On the Cisco ASR 1004 and Cisco ASR 1006 routers, the Cisco ASR1000-RP1 is supported as a modular component and supports two memory options:

- 2-GB DRAM
- 4-GB DRAM

The Cisco ASR 1006 Router contains two RP slots to support full hardware redundancy for RP1s within the same router.

For information about the Cisco ASR1000-RP1, see the following document:

Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/install/guide/asr1routers/asr1higV8.html

Cisco ASR 1000 SPA Interface Processor

The Cisco ASR 1000 Series SPA Interface Processor (SIP) (Cisco ASR1000-SIP10) accepts up to 4 half-height or 2 full-height Cisco SPAs, including Ethernet, Packet over SONET/SDH (POS), and Serial SPAs, providing up to 10-Gbps connection to the system backplane with an ability to differentiate traffic based on Layer 2 or Layer 3 header information.

The Cisco ASR 1000 Series SIP is built into the Cisco ASR1002 chassis and supported as a modular component on the Cisco ASR1004 and Cisco ASR1006 chassis. The Cisco ASR 1004 chassis contains two SIP slots; the Cisco ASR 1006 chassis contains three SIP slots.

For information about the Cisco ASR 1000 Series SIP, see the following documents:

- *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide* at the following location:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/ASR1000/asr_sip_spa_hw.html

- *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guid*e at the following location:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ASR1000/ASRspasw.html

Shared Port Adapters

Shared Port Adapters (SPAs) provide the physical interfaces for router connectivity ranging from copper, channelized, POS, and Ethernet.

The Cisco ASR 1000 Series Routers support the following SPAs:

Serial SPAs

- 2-Port and 4-Port T3/E3 Serial SPA (SPA-2XT3/E3, SPA-4XT3/E3)
- 2-Port and 4-Port Channelized T3 SPA (SPA-2XCT3/DS0, SPA-4XCT3/DS0)
- 8-Port Channelized T1/E1 Serial SPA (SPA-8XCHT1/E1)
- 4-Port Serial Interface SPA (SPA-4XT-Serial)

Ethernet SPAs

- 4-Port and 8-Port Fast Ethernet SPA (SPA-4X1FE-TX-V2, SPA-8X1FE-TX-V2)
- 1-Port 10-Gigabit Ethernet SPA (SPA-1X10GE-L-V2)
- 2-Port Gigabit Ethernet SPA (SPA-2X1GE-V2)
- 5-Port Gigabit Ethernet SPA (SPA-5X1GE-V2)
- 8-Port Gigabit Ethernet SPA (SPA-8X1GE-V2)
- 10-Port Gigabit Ethernet SPA (SPA-10X1GE-V2)

POS SPAs

- 1-Port OC-12c/STM-4 POS SPA (SPA-1XOC12-POS)
- 2-Port and 4-Port OC-3 POS SPA (SPA-2XOC3-POS, SPA-4XOC3-POS)

For information about the SPAs supported on the Cisco ASR 1000 Series Routers, see the following documents:

- *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide* at the following location:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/ASR1000/asr_sip_spa_hw.html

- *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide* at the following location:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ASR1000/ASRspasw.html

1GB USB Flash Token for Cisco ASR 1000 Series

The Cisco ASR 1000 Series Routers support a 1GB USB Flash Token for Cisco ASR 1000 Series. This USB Flash token can be used to store images, configuration files, or any other type of data, and can also be used to boot a consolidated package on the router. (The USB Flash token can not be used to boot sub-packages on the router.)

Caution Only Cisco ASR 1000 RP1 1GB USB flash memory (the 1GB USB Flash Token for Cisco ASR 1000 Series) is supported for use with the Cisco ASR 1000 Series Routers.

New Software Features in Cisco IOS XE Release 2.1.0

This section describes new and changed features in Cisco IOS XE Release 2.1.0. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS XE Release 2.1.0. To determine if a feature is new or changed, refer to the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Note This section is not cumulative and list only new features that were introduced for Cisco IOS XE Release 2.1.0. For information about inherited features, refer to the Cisco Feature Navigator tool at http://www.cisco.com/go/fn.

- BFD IPv6 Encaps Support
- BFD—IPv6 Static Route Support
- DHCP—DHCPv6 Relay Agent Notification for Prefix Delegation
- DHCP Relay Server ID Override and Link Selection Option 82 Suboptions
- DHCPv6 Ethernet Remote ID Option
- Integrated Session Border Controller
- IPv6: Base Protocols High Availability
- IPv6: NSF and Graceful Restart for MP-BGP IPv6 Address Family
- IPv6: RIPng Non-Stop Forwarding
- IPv6: Static Route Non-Stop Forwarding
- MQC—Distribution of Remaining Bandwidth Using Ratio
- PPPoE Session Limit Local Override
- Quality of Service for Gigabit EtherChannels
- QoS: Policies Aggregation
- TCP MIB for RFC4022 Support
- VLAN Mapping to GEC Member Links

BFD IPv6 Encaps Support

The Bidirectional Forwarding Detection for IPv6 (BFDv6) protocol provides fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. The BFD IPv6 Encaps Support feature updates the Bidirectional Forwarding Protocol (BFD) protocol to provide IPv6 support and accommodate IPv6 addresses.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-bfd.html

BFD—IPv6 Static Route Support

The BFD—IPv6 Static Route Support feature enables BFD for IPv6 to be used to verify next-hop reachability for IPv6 static routes.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-bfd.html

DHCP—DHCPv6 Relay Agent Notification for Prefix Delegation

The DHCP—DHCPv6 Relay Agent Notification for Prefix Delegation feature allows the router working as a DHCPv6 relay agent to find prefix delegation options by reviewing the contents of a DHCPv6 packet that is being relayed by the relay agent to the client.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dhcp.html

DHCP Relay Server ID Override and Link Selection Option 82 Suboptions

The DHCP Relay Server ID Override and Link Selection Option 82 Suboptions feature enables the relay agent to be part of all DHCP message exchanges by supporting the use of two suboptions of the relay agent information option (option 82). This design allows DHCPv4 to operate in networks where direct communication between the client and server is not possible or desired. When used together, these two suboptions enable the deployment of an architecture where it is desirable to have all DHCP traffic flow through the relay agent, allowing for greater control of DHCP communications.

This feature also introduces the capability to manually configure the interface for the relay agent to use as the source IP address for messages relayed to the DHCP server. This configuration allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface).

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcpservidlink_mcp.html

DHCPv6 Ethernet Remote ID Option

The DHCPv6 Ethernet Remote ID Option feature adds the remote-ID option to relayed (RELAY-FORWARD) DHCPv6 packets.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dhcp.html

Integrated Session Border Controller

The Integrated Session Border Controller (SBC) is introduced on the Cisco ASR 1000 Series Routers. The Integrated SBC is integrated with other features on the Cisco ASR 1000 Series Routers, without requiring additional application-specific hardware, such as service blades, or the need to create an overlay network of standalone SBC appliances.

Session border controllers are used as key components in interconnecting Voice over IP (VoIP) and multimedia networks of different enterprise customers and service providers. SBCs are deployed at the edge of networks to meet the need for secure, intelligent border element functions. Using SBCs, the end user can make voice and video calls to another end user without being concerned about protocols, network reachability, or safety of the network.

The SBC enables direct IP-to-IP interconnect between multiple administrative domains for session-based services providing protocol and signaling interworking, security, Quality of Service (QoS), network hiding, statistics gathering, and admission control and management.

Currently the data border element (DBE) functionality of the Integrated Session Border Controller is supported on the Cisco ASR 1000 Series Routers.

For information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbc/2_xe/sbc_2_xe_book.html

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

IPv6: Base Protocols High Availability

The IPv6: Base Protocols High Availability feature enables IPv6 neighbor discovery to support stateful switchover.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-mptcl_bgp.html

IPv6: NSF and Graceful Restart for MP-BGP IPv6 Address Family

The IPv6: NSF and Graceful Restart for MP-BGP IPv6 Address Family feature adds graceful restart capability support for IPv6 BGP unicast, multicast, and VPNv6 address families, enabling Cisco nonstop forwarding (NSF) functionality for BGP IPv6. The BGP graceful restart capability allows the BGP routing table to be recovered from peers without keeping the TCP state.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-mptcl_bgp.html

IPv6: RIPng Non-Stop Forwarding

The IPv6: RIPng Non-Stop Forwarding feature enables IPv6 RIP to support nonstop forwarding.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-rip.html

IPv6: Static Route Non-Stop Forwarding

The IPv6: Static Route Non-Stop Forwarding feature enables IPv6 static routes to support nonstop forwarding.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes.html

MQC—Distribution of Remaining Bandwidth Using Ratio

The MQC—Distribution of Remaining Bandwidth Using Ratio feature allows service providers to configure a bandwidth-remaining ratio on subinterfaces and class queues. This ratio specifies the relative weight of a subinterface or queue with respect to other subinterfaces or queues. During congestion, the router uses this bandwidth-remaining ratio to determine the amount of excess bandwidth (unused by priority traffic) to allocate to a class of nonpriority traffic.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/bwdth_remain_ratio.html

PPPoE Session Limit Local Override

The PPPoE Session Limit Local Override feature enables the session limit configured locally on the broadband remote access server (BRAS) or L2TP access concentrator (LAC) to override the per-NAS-port session limit downloaded from the RADIUS server when Subscriber Service Switch (SSS) preauthorization is enabled.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/bbdsl/configuration/guide/bba_ppoe_sllov.html

Quality of Service for Gigabit EtherChannels

The Quality of Service: Policies Aggregation feature allows the default traffic classes of different policy maps on the same physical interface to be configured as a single traffic class within the Modular QoS CLI. The Quality of Service for Gigabit EtherChannels feature extends the functionality introduced in the Quality of Service: Policies Aggregation feature by allowing the default traffic classes of different member links in the same Gigabit EtherChannel bundle to be configured as a single traffic class within the Modular QoS CLI.

This feature is documented as part of the Quality of Service: Policies Aggregation feature.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_policies_agg.html

QoS: Policies Aggregation

The QoS: Policies Aggregation feature allows the default traffic classes of different policy maps on the same physical interface to be configured as a single traffic class within the Modular QoS CLI.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_policies_agg.html

TCP MIB for RFC4022 Support

The TCP MIB for RFC 4022 Support feature introduces support for RFC 4022, *Management Information Base for the Transmission Control Protocol (TCP)*. RFC 4022 is an incremental change of the TCP MIB to improve the manageability of TCP.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://www.cisco.com/go/mibs

VLAN Mapping to GEC Member Links

The VLAN Mapping to GEC Member Links feature allows for the static assignment of user traffic as identified by a VLAN ID to a given member link of a GEC bundle. Network administrators can manually assign VLAN subinterfaces to a primary and secondary link. Load balancing to downstream equipment can be configured, regardless of the downstream equipment capabilities, and will provide failover protection by redirecting traffic to the secondary member link if the primary link fails. Member links are supported with up to 16 bundles per chassis.

For information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/lanswitch/configuration/guide/lsw_cfg_gecvlan.html

Release Note Only Software Features in Cisco IOS XE Release 2.1.0

This section describes features that are supported in Cisco IOS XE Release 2.1.0 but that are documented only in the release notes and do not have a link to a feature module. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS XE Release 2.1.0.

- 8-Way CEF Load Balancing
- BGP Reduction in Transient Memory Usage
- CEF Support for IP Routing Between IEEE 802.1 Q VLANs
- Class-Based Quality of Service Management Information Base
- Compression Control
- DLR Enhancements: PGM RFC-3208 Compliance
- Frame Relay FRF.1.2 Annex A Support
- Interfaces MIB: SNMP Context Based Access
- ISSU - IGMP Snooping
- NAT—Performance Enhancement - Translation Table Optimization
- Parse Bookmarks
- PPPoE Over Gigabit Ethernet Interface
- RADIUS Attribute 52 and 53 Gigaword Support
- RADIUS Attribute 77 for DSL
- Selective Packet Discard (SPD)
- TCP MIB for RFC4022 Support
- VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP

8-Way CEF Load Balancing

Destination IP prefixes are added to the routing table by routing protocols or static routes. Each path is a valid route to reach the destination prefix. The set of active paths is the set of paths with the best cost. Cisco Express Forwarding load balancing is the ability to share the traffic to a destination prefix over up to eight active paths (an increase from the previous support of six active paths). Load among the active paths can be distributed per destination.

BGP Reduction in Transient Memory Usage

The BGP Reduction in Transient Memory Usage feature implements a reduction in transient memory usage by BGP when BGP updates are built in Cisco IOS XE Release 2.

CEF Support for IP Routing Between IEEE 802.1 Q VLANs

Cisco Express Forwarding (CEF) is supported on interfaces on which IEEE 802.1Q encapsulation has been enabled at the subinterface level. You no longer have to disable CEF operation on interfaces that are using IEEE 802.1Q encapsulation on VLAN subinterfaces.

Class-Based Quality of Service Management Information Base

The Class-Based Quality of Service Management Information Base (Class-Based QoS MIB) provides read access to class-based QoS configurations. This MIB also provides QoS statistics information based on the Modular QoS CLI, including information regarding class map and policy map parameters.

This Class-Based QoS MIB is actually two MIBs: CISCO-CLASS-BASED-QOS-MIB and CISCO-CLASS-BASED-QOS-CAPABILITY-MIB.

Compression Control

The PPP Compression Control Protocol (CCP) defines a method for negotiating data compression over PPP links. These links can be either leased lines or circuit switched WAN links such as ISDN. PPP CCP allows vendors to support multiple data compression algorithms.

DLR Enhancements: PGM RFC-3208 Compliance

In compliance with RFC 3208, the DLR Enhancements: PGM RFC-3208 Compliance feature adds off-tree designated local repairer (DLR) support and redirecting poll response (POLR) capability for upstream DLRs to the Cisco implementation of Pragmatic General Multicast (PGM).

Frame Relay FRF.1.2 Annex A Support

The FRF.1.2 Annex A Support feature is also called Local Management Interface (LMI) segmentation. It supports an enhancement to the Frame Relay LMI protocol where LMI full status messages are segmented because of MTU constraints or large numbers of permanent virtual circuits (PVCs). This feature is useful when the maximum MTU size is insufficient to accommodate the large number of PVCs on the link. During Frame Relay internetworking with other Layer 2 protocols, the MTUs on each interface must match. In software without the FRF.1.2 Annex A Support feature, you cannot change the MTU size on the Frame Relay side and place all PVC data into one LMI packet. The FRF.1.2 Annex A Support feature removes this limitation.

The FRF.1.2 Annex A standard adds a new message type “Full status continued” to an LMI packet. When a DCE determines that it cannot fit all PVCs into one packet (enforced by the MTU size), the message type is set to “Full status continued.” The DTE responds to “Full status continued” messages that are sent to this packet immediately instead of waiting for the T391 timer to expire. The DCE sends the remaining PVCs in one or more “Full status continued” messages until all the remaining PVCs can fit into one message. At this point, a normal “Full status” message is sent.

If the DTE receives a “Full status” or “Full status continued” STATUS message in response to a “Full status continued” STATUS ENQUIRY message, this exchange indicates a lower-valued data-link connection identifier (DLCI) than the prior “Full status continued” STATUS message (and is considered to be an error event), and PVC information elements (IEs) are not processed. The next time the T391 timer expires, the “Full status” STATUS ENQUIRY procedure is reinitiated.

This feature follows the FRF.1.2 implement agreement [1] and allows Cisco IOS software to be compliant with the FRF.1.2 standard. The implementation is platform-independent and applies to all platforms running Cisco IOS software that support Frame Relay. This feature interoperates only with existing Cisco IOS software releases where all PVCs can be reported in one packet. A router running the new functionality must be able to interoperate with routers running existing Cisco IOS software releases and with routers that support the new functionality using the continuation status request and reply frames. Only LMI types Q.933A and ANSI support the FRF.1.2 Annex A standard.

You can track “Full status continued” packets by using the **debug frame-relay lmi** command in privileged EXEC mode. An extra field, 04, has been added to the display output. The following example indicates where in the report to look for this field (the text is in **bold** for this example):

```
17:42:39: Serial1(out): StEnq, myseq 126, yourseen 125, DTE up
17:42:39: datagramstart = 0x40058DA4, datagramsize = 13
17:42:39: FR encap = 0x00010308
17:42:39: 00 75 51 01 04 53 02 7E 7D
```

The string segment “active/inactive” in the display of the **show interface** commands indicates whether the FRF.1.2 Annex A standard is triggered. The report indicates active when routers receive the “Full status continued” message; otherwise, the report indicates inactive.

Interfaces MIB: SNMP Context Based Access

The Interfaces MIB (IF-MIB) has been modified to support context-aware packet information in Virtual Route Forwarding (VRF) environments. VRF environments require that contexts apply to Virtual Private Networks (VPNs) so that clients can be given selective access to the information stored in the IF-MIB. Clients that belong to a particular VRF can access information about the interface from the IF-MIB that belongs to that VRF only. When a client tries to get information from an interface that is associated with a particular context, the client can see only the information that belongs to that context and cannot see IF-MIB information that is associated with interfaces that are connected to another VRF to which it is not entitled. No commands have been modified or added to support this feature.

The IF-MIB supports all tables that are defined in RFC 2863 and the CISCO-IFEXTENSION-MIB.

ISSU - IGMP Snooping

This ISSU - IGMP Snooping feature adds ISSU support for IGMP Snooping.

NAT—Performance Enhancement - Translation Table Optimization

The NAT - Performance Enhancement - Translation Table Optimization feature provides greater structure for storing translation table entries and an optimized look up in the table for associating table entries to IP connections.

Parse Bookmarks

The Parse Bookmarks feature quickly processes consecutive similar commands, such as access-lists and prefix-lists, up to five times faster. The Parse Bookmarks feature reduces boot time and load time for large configurations with many similar consecutive commands. This feature is an enhancement to the parsing algorithm; therefore no configuration changes are needed.

PPPoE Over Gigabit Ethernet Interface

The PPPoE over Gigabit Ethernet Interface feature enhances PPP over Ethernet (PPPoE) functionality by adding support for PPPoE and PPPoE over IEEE 802.1Q VLANs on Gigabit Ethernet interfaces.

RADIUS Attribute 52 and 53 Gigaword Support

The RADIUS Attribute 52 and Attribute 53 Gigaword Support feature introduces support for Attribute 52 (Acct-Input-Gigawords) and Attribute 53 (Acct-Output-Gigawords) in accordance with RFC 2869. Attribute 52 keeps track of the number of times the Acct-Input-Octets counter has rolled over the 32-bit integer throughout the course of the provided service; attribute 53 keeps track of the number of times the Acct-Output-Octets counter has rolled over the 32-bit integer throughout the delivery of service. Both attributes can be present only in Accounting-Request records where the Acct-Status-Type is set to “Stop” or “Interim-Update.” These attributes can be used to keep accurate track of and bill for usage.

RADIUS Attribute 77 for DSL

The RADIUS Attribute 77 for DSL feature introduces support for attribute 77 (Connect-Info) to carry the textual name of the virtual circuit class associated with the given permanent virtual circuit (PVC). (Although attribute 77 does not carry the unspecified bit rate (UBR), the UBR can be inferred from the classname used if one UBR is set up on each class.) Attribute 77 is sent from the network access server (NAS) to the RADIUS server via Accounting-Request and Accounting-Response packets.

Selective Packet Discard (SPD)

When in severe overload conditions, routers that cannot keep up with the incoming packet stream must drop packets. If no intelligence is applied to choosing which ones to discard, this will impact the stability of routing protocols. This feature applies some simple choices to selectively discard packets likely to be unimportant for routing and interface stability. SPD is enabled by default; there are no commands or configuration tasks required.

TCP MIB for RFC4022 Support

The TCP MIB for RFC 4022 Support feature introduces support for RFC 4022, *Management Information Base for the Transmission Control Protocol (TCP)*. RFC 4022 is an incremental change of the TCP MIB to improve the manageability of TCP.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://www.cisco.com/go/mibs

VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP

The VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP feature introduces support to make the following RADIUS attributes VRF aware: attribute 22 (Framed-Route), a combination of attribute 8 (Framed-IP-Address) and attribute 9 (Framed-IP-Netmask), and the Cisco VSA route command. Thus, static IP routes can be applied to a particular VRF routing table rather than the global routing table.

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

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:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

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 this URL:

http://tools.cisco.com/RPF/register/register.do

The Cisco ASR 1000 Series Routers support the following verified MIBs:

- ATM-MIB
- BGP4-MIB (RFC-1657)
- CISCO-AAA-SERVER-MIB
- CISCO-AAA-SESSION-MIB
- CISCO-AAL5-MIB
- CISCO-ATM-EXT-MIB
- CISCO-BGP4-MIB
- CISCO-BGP-POLICY-ACCOUNTING-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-CONTEXT-MAPPING-MIB
- CISCO-DATA-COLLECTION-MIB
- CISCO-EMBEDDED-EVENT-MGR-MIB

- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-ENTITY-EXT-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-SENSOR-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-FLASH-MIB
- CISCO-FRAME-RELAY-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-HSRP-MIB
- CISCO-HSRP-EXT-MIB
- CISCO-IETF-ATM-PVCTRAP-EXTN-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-MIB
- CISCO-IETF-PW-ATM-MIB
- CISCO-IETF-PW-MPLS-MIB
- CISCO-IF-EXTENSION-MIB
- CISCO-IMAGE-MIB
- CISCO-IP-LOCAL-POOL-MIB
- CISCO-IP-URPF-MIB
- CISCO-IPMROUTE-MIB
- CISCO-IPSEC-MIB
- CISCO-IPSEC-FLOW-MONITORING-MIB
- CISCO-IPSEC-POLICY-MAP-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-MIBCISCO-SLB-MIB
- CISCO-SLB-EXT-MIB
- CISCO-SONET-MIB
- CISCO-SYSLOG-MIB
- CISCO-VLAN-IF-RELATIONSHIP-MIB
- CISCO-VLAN-MEMBERSHIP-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-2665, 3635)
- EVENT-MIB (RFC-2981)
- EXPRESSION-MIB (early draft of RFC-2982)
- FRAME-RELAY-DTE-MIB (RFC-1315)
- IF-MIB (RFC-2863)
- IGMP-STD-MIB (RFC-2933)
- IP-FORWARD-MIB (RFC- 4292)
- 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-3031)
- MPLS-VPN-MIB
- MSDP-MIB
- NOTIFICATION-LOG-MIB (RFC-3014)
- OSPF-MIB (RFC-1850)
- OSPF-TRAP-MIB (RFC-1850)
- PIM-MIB (RFC- 2934)
- RMON (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)
- 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 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 Management Information Base (MIB) protocol, see the following document:

Cisco ASR 1000 Series Aggregation Services Routers MIB Specifications Guide at the following location:

http://www.cisco.com/en/US/docs/routers/asr1000/mib/guide/asr1kmib.html

Limitations and Restrictions

This section lists the limitations and restrictions that apply to the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2 and contains the following sections:

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.

Note The User-Defined Parent Class Limitation (for Hierarchical QoS) is no longer applicable in Cisco IOS XE Release 2.3.1 and later releases. The use of a single child policy map in multiple instances in the definition of a user-defined parent class is supported in these later releases.

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.

Tunnel Protection+ Priority Queuing Limitation

On a Cisco ASR 1000 Series Router configured with the **tunnel protection** command (which applies to DMVPN, VTI and GRE) and priority queuing (which applies to the outbound physical interface for the tunnel), it is not possible to oversubscribe the encryption coprocessor and maintain low latency traffic. A possible workaround is to apply both the crypto and priority qos policy to the physical interface. For more details, see CSCsy94190.

Starting with Cisco IOS XE Release 2.4.1, the **platform ipsec llq qos-group** command resolves the preceding limitation. See the "IPSec QoS Group-Based LLQ QoS" section on page 71.

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 on 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) per Cisco ASR 1000 Series chassis in Cisco IOS XE Release 2.2.3 and later releases are as follows:

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

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 for 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. CoPP does support packet matching with access lists, therefore you can police Layer 2 Tunneling Protocol (L2TP) and Dynamic Host Configuration Protocol (DHCP) packets matched by access lists. For example, L2TP and DHCP packets can be matched with access lists that check User Datagram Protocol (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 for Cisco IOS XE Release 2.2.1:

- Table 13 describes the functionality supported in the Raw FPM an d Basic FPM (Raw FPM+) modes in Cisco IOS XE Release 2.2.1:

Table 13 FPM Functionality Support by Mode

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

- 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 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.

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 Beginning with Cisco IOS XE Release 2.1.1 and later releases, up to 4K IPSec tunnels are supported 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 Beginning with Cisco IOS XE Release 2.2.3 and later releases, the MLP scaling limits have been revised. For the revised scaling limits for Cisco IOS XE Release 2.2.3 and later releases, see "Scaling Limits for MLP" section on page 143.

Important Notes

The following sections contain important notes about Cisco IOS XE Release 2 and later releases that can apply to the Cisco ASR 1000 Series Routers.

Deferrals

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

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

Field Notices and Bulletins

- Field Notices—Cisco recommends that you view the field notices for this release to see if 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.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.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 on Cisco IOS IPSec commands, see the Cisco IOS Security Command Reference at: http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_s5.html

- 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 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 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.

- 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 find the matrix at

http://www.cisco.com/en/US/docs/routers/asr1000/technical_references/asr1000alg_support.pdf

Important Notes in Cisco IOS XE Release 2.6.0:

This section describes important issues that you should be aware of for 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 \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:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/legacy_qos_cli_deprecation_xe.html

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 issues that you should be aware of for 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.

In a GRE over IPsec configuration with a crypto map configured on the physical interface, traffic shaping on the GRE tunnel interface is not supported. The workaround is to use sVTI (tunnel protection with tunnel mode IPsec).

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 described in the "Configuring NAT for IP Address Conservation" module.

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 the "IP Access List Sequence Numbering" document at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsaclseq.htm

Note 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 2.4.2t:

This section describes important issues that you should be aware of for Cisco IOS XE Release 2.4.2t. Due to the Certification Authorities requirements access to the platform shell in this FIPS 140-2 certified version of IOS XE is disabled by invalidating the "platform shell" CLI command:

```
mcp-4ru-28(config)#platform ?
  ipsec      Platform specific ipsec command
  multicast  Configure multicast
  reload     Platform specific reload command
  shell      Control platform shell access command availability
mcp-4ru-28(config)#platform shell
%Invalid command
```

For additoinal information about how to request platform shell access, please refer to the "Command Reference Guide" at the following URL:

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_r1.html#wp1071157

Important Notes in Cisco IOS XE Release 2.3.0

This section describes important issues that you should be aware of for 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 issues that you should be aware of for 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 issues that you should be aware of for 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 in Cisco IOS XE Release 2.1.1

This section describes important issues that you should be aware of for 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        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-confg]? /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 issues that you should be aware of for Cisco IOS XE Release 2.1.0 and later releases.

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

Table 14 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. Please consult 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 14 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 14 High Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers

Major Feature Category	Features Not Supported
ATM	
	Support for ATM features begins in Cisco IOS XE Release 2.3.0. No ATM features are supported in earlier releases.
Broadband	
	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)
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

Table 14 High Level Feature Sets Not Supported for the Cisco ASR 1000 Series Routers (continued)

Major Feature Category	Features Not Supported
	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
	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.

Caveats

See the Caveats for Cisco IOS XE Release 2 at “Caveats for Cisco IOS XE Release 2” section on page 167.

Related Documentation

The following sections describe the documentation available for the Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2. These documents consist of hardware and software installation guides, system error message documentation, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com.

Use these release notes with these documents and tools:

Platform-Specific Documents

The following platform-specific documents are available for the Cisco ASR 1000 Series Routers on Cisco.com:

- *Cisco ASR 1000 Series Aggregation Services Routers Documentation Roadmap*

  Provides an online directory to quickly access publications for the Cisco ASR 1000 Series Routers.

  http://www.cisco.com/en/US/docs/routers/asr1000/roadmap/asr1000rm.html

- *Cisco ASR 1002 Quick Start Guide*

  Provides a summary of the hardware installation guide for the Cisco ASR 1002 Router.

  http://www.cisco.com/en/US/docs/routers/asr1000/quick/start/guide/asr1_qs2.html

- *Cisco ASR 1002-F Quick Start Guide*

  Provides a summary of the hardware installation guide for the Cisco ASR 1002 Router.

  http://www.cisco.com/en/US/docs/routers/asr1000/quick/start/guide/asr1_qs2F.html

- *Cisco ASR 1004 Quick Start Guide*

  Provides a summary of the hardware installation guide for the Cisco ASR 1004 Router.

  http://www.cisco.com/en/US/docs/routers/asr1000/quick/start/guide/asr1_qs4.html

- *Cisco ASR 1006 Quick Start Guide*

  Provides a summary of the hardware installation guide for the Cisco ASR 1006 Router.

  http://www.cisco.com/en/US/docs/routers/asr1000/quick/start/guide/asr1_qs6.html

- *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).

  http://www.cisco.com/en/US/docs/routers/asr1000/install/guide/asr1routers/asr1higV8.html

- *Upgrading to the Cisco ASR 1000 Series Routers ROMmon Image Release 12.2(33r)XND*

  Contains procedures for downloading independent ROM monitor (ROMmon) Release 12.2(33r)XND software onto the Route Processors (RPs), Embedded Services Processors (ESPs), and Shared Port Adapter Interface Processors (SIPs) on the Cisco ASR 1000 Series Routers.

  http://www.cisco.com/en/US/docs/routers/asr1000/rommon/33xnd_rommon.html

- *Upgrading to the Cisco ASR 1000 Series Routers ROMmon Image Release 12.2(33r)XNC0*

  Contains procedures for downloading independent ROM monitor (ROMmon) software onto the Route Processor 2 (RP2) on a Cisco ASR 1000 Series Router.

  http://www.cisco.com/en/US/docs/routers/asr1000/rommon/33xnc0_rommon.html

- *Upgrading to the Cisco ASR 1000 Series Routers ROMmon Image Release 12.2(33r)XNB*

Contains procedures for downloading independent ROM monitor (ROMmon) Release 12.2(33r)XNB software onto the Route Processors (RPs), Embedded Services Processors (ESPs), and Shared Port Adapter Interface Processors (SIPs) on the Cisco ASR 1000 Series Routers.

http://www.cisco.com/en/US/docs/routers/asr1000/rommon/33xnb_rommon.html

- *Upgrading to the Cisco ASR 1000 Series Routers ROMmon Image Release 12.2(33r)XN2*

  Contains procedures for downloading independent ROM monitor (ROMmon) Release 12.2(33r)XN2 software onto the Route Processors (RPs), Embedded Services Processors (ESPs), and Shared Port Adapter Interface Processors (SIPs) on the Cisco ASR 1000 Series Routers.

  http://www.cisco.com/en/US/docs/routers/asr1000/rommon/33xn2_rommon.html

- *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.

  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/asrswcfg.html

- *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.

  http://www.cisco.com/en/US/docs/routers/asr1000/operations/guide/asr1000ops.html

- *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.

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/ASR1000/asr_sip_spa_hw.html

- *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.

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ASR1000/ASRspasw.html

- *Cisco ASR 1000 Series Aggregation Services Routers MIB Specifications Guide*

  Describes Cisco ASR 1000 Series Routers product implementation of the Management Information Base (MIB) protocol.

  http://www.cisco.com/en/US/docs/routers/asr1000/mib/guide/asr1kmib.html

- *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.

  http://www.cisco.com/en/US/partner/docs/routers/asr1000/feature/guides/ASR_depop.html

- *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model*

  Describes the Cisco Unified Border Element (SP Edition) functions, features, and configuration tasks. The name Cisco Unified Border Element (SP Edition) replaces the Integrated Session Border Controller name. Introduces the unified model and a new unified feature set supported in

Cisco IOS XE Release 2.4 on the Cisco Unified Border Element (SP Edition). A comprehensive guide for the Cisco Unified Border Element (SP Edition) feature on the Cisco ASR 1000 Series Routers.

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/2_xe/sbcu_2_xe_book.html

- *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model*

  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.

  http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

- *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.

  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbc/2_xe/sbc_2_xe_book.html

- *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.

  http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

- *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.

  http://www.cisco.com/en/US/docs/routers/asr1000/technical_references/asr1000alg_support.pdf

- *Cisco IOS XE System Message Guide*

  Describes non-IOS messages specific to the Cisco ASR 1000 Series Routers.

  http://www.cisco.com/en/US/docs/routers/asr1000/system/messages/guide/xemsg.html

- *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.

  http://www.cisco.com/en/US/docs/routers/asr1000/rcsi/asr1rcsi.html

On Cisco.com at:

Products and Services: Routers: Cisco ASR 1000 Series Aggregation Services 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 URL:

http://www.cisco.com/go/fn

Error Message Documentation for Cisco IOS XE Release 2

Information about error messages for Cisco IOS XE Release 2 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.

  http://www.cisco.com/en/US/docs/routers/asr1000/system/messages/guide/xemsg.html

- *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 sub-package in Cisco IOS XE Release 2.

  http://www.cisco.com/en/US/docs/ios/12_2sb/system/messages/sys_msg_book.html

- *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 sub-package in Cisco IOS XE Release 2.

  http://www.cisco.com/en/US/docs/ios/12_2sr/system/messages/122srsms.html

- 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 Software Documentation Set

The Cisco IOS XE software documentation set consists of configuration guides and Cisco IOS command references.

The configuration guides are consolidated platform-independent configuration guides by technology for the Cisco IOS XE release train. The command references are generic and support all Cisco platforms and all Cisco IOS and Cisco IOS XE releases.

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 or the Cisco ASR 1000 Series Aggregation Services Routers.** For the latest feature information and caveats for Cisco IOS XE Release 2, see the New and Changed

Information section and the Caveats for Cisco IOS XE Release 2 section of these release notes. Additionally, 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

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN

NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

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:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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.

Release 2.6 Caveats

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

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

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

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

This section consists of the following subsections:

Open Caveats—Cisco IOS XE Release 2.6.2

This section documents possible unexpected behavior by Cisco IOS XE Release 2.6.2

- CSCsu59515

  Telnet inside host from outside the host fails when port 23 is statically allocated on a Cisco ASR 1000 Router.

  Workaround: None

- CSCtc05275

  On a Cisco ASR 1000 Router a false memory leak has been seen within the AAA Memory Stats Tool.

  When there are multiple separately allocated attribute lists attached to a request or and event in AAA, the memory stats tool gives wrong information, as it does not account for all the separate lists after freeing the event with the request.

  Workaround: None

- CSCtc18663

  When running PPPoEoA PTA, one may see some ATM VCs stay in inactive state on a Cisco ASR 1000 Router.

  This condition may occur when loading this configuration while bring up the ATM SPA.

  Workaround: Is to do a **shut** and then a **no shut** on the interface this should allow for all the ATM VCs to come up.

- CSCtc45832

  When tracking stops the data-plane logs out of the PKT-MEM trace log this problem will occur on an ASR 1000 Router Series the sessions will be dropped and the QoS hierarchy will shut down. There also will be pending queue objects waiting to be flushed out in the list.

  The following command will show the BQS RM status:

show plat hard qfp act inf bqs stat

In rare conditions, an error may occur for extreme over-subscribed enviroments. When sending 10G (For example: 5G as priority, and 5G as non-priority) traffic to a 1G interface.

All priority and control packets are dropped by the hardware this occur when the packet buffers are depleted; and when the schedule stops forwarding output packets

Workaround: There is no known workaround to this problem.

- CSCtc69297

  Tracebacks has been seen with cli **sh platform hardware qfp active** feature acl tree on the Cisco ASR 1000 Router.

  This condition has been seen, when there are a huge number of acls configured on the router.

  Workaround: None

- CSCtc76606

  The following error message has been observed on the console, when the SPA is out of sync:

  SPA_OIR-3-OUT_OF_SYNC

  Workaround: None

- CSCtc86844

  Idmgr invalid error messages has been seen on a Cisco ASR 1000 Router console.

  This instance has been observed after the router has scaled to 32k PPPoL2TP sessions and running traffic with events. However, there are no impact on the router.

  Workaround: None

- CSCtc90106

  Memory leaks are seen when changing the **"fvrf"** during traffic flow in the IPSEC_RMAL process on a Cisco ASR 1000 Router. This condition has been observed when changing **"fvrf"** to show as **"fvrf2"**, while sending traffic and checking incremental memory leaks the memory leaks are the seen on the router.

  Workaround: Do not change fvrf's frequently.

- CSCtc91018

  On a Cisco ASR 1000 Router the subinterface counters with Frame Relay Encapsulation can show higher values than the counters on the main interface, when self-pinging the subinterface.

  Workaround: None

- CSCtd08709

  When one LTS is restricted with CAC calls are not terminating through another LTS.

  After configuring call admission control on LTS2 to 1 and making 20 calls through LAC all are go to LTS2 as per the priority, and as call admission configured on LTS2 call should be diverted back to LAC and should terminated on LTS1 which is not happening.

  Workaround: Do not restrict call admission control on LTS.

- 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: None

- CSCtd36301

  At every session churning of IPv6 PPPoE uses more prefixes for same tunnel and session value. No used IPv6 Prefixes in local IPv6 pool are incremented at every session flap iteration in IPv6 LNS for same tunnel and session value.

  This instance may happen, when Local IPv6 prefix pool is used to assign ipv6 address and the sessions are churning at a flap rate of 70 sessions per seconds for 8000 sessions.

  Workaround: None

- CSCtd37057

  On a heavily loaded Cisco ASR 1000 Router Series, rapid QoS queuing configuration changes involving the removal of existing configuration and addition of new configuration could cause the system to experience temporary resource outage.

  The conditions under which this has been observed involve 32000 flapping PPPoE sessions combined with configuration changes on the system.

  Workaround: Avoiding rapid and large QoS configuration changes on a heavily loaded system will avoid the problem reported in this caveat.

- CSCtd80542

  Loop observed, when configuring SNMP bulk mib walk. The loop has been observed at tunnelInetConfigIfIndex.

  This condition has occurred, when scaled configuration includes tunnel interface 2147483647.

  Workaround: None

- CSCtd83379

  DHCP discover packets are not reaching the server via a Bridge from the client.

  This condition have been seen when the Pagent Client is initiating DHCP discover message to the server via the Relay.

  The Relay (ASR 1002) is using the unnumber interface to forward the DHCP discover packets to the server. The Bridge to Bridge between Ethernet and serial interfaces are using the same bridge group.

  It has been seen that the DHCP discover packets are reaching up to the Bridge interface and the Relay unnumber interface is not receiving the DHCP discover packet.

  Workaround: No workaround.

- CSCtd87072

  IOSD will restart, when changing tunneling mode in scaled IPSec Sessions on an ASR 1000 Router Series.

  This condition has been observed, after IOSD restarts the tunneling mode has changed in a scaled IPSec Session enviroment.

  Workaround: None

- CSCtd91950

  A Cisco ASR 1000 Router Series with the Lawful Intercept feature configured may reset unexpectedly under certain conditions when streams are modified**/disabled/re-enabled** during traffic flow.

  The conditions necessary for this situation to be encountered are multiple MDs, configuration of circuit-id based pre-provisioned stream entries and active PPPoE sessions.

  Workaround: There are no known workarounds.

- CSCtd98510

  Some of the L2TPv3 Xconnects are not coming up after repeated (5-6) switchovers and OIR.

  This instance may occur when an AC is down while sessions are in local state and are not ready.

  Workaround: Is to clear L2TP to recover from this problem.

- CSCte43453

  QoS accounting Interim record for the parent policy-map class-default class has incorrect packets and bytes stats while under traffic load.

  This condition has been seen when PTA session with Model D2.2 QoS has been enabled. QoS accounting has been enabled at the parent policy-map class-default class. While under traffic load, the accounting Interim record has incorrect stats as compared to the QoS stats in the output of show policy-map session.

  Workaround: None

- CSCte46896

  Following traceback appears on the a Cisco ASR 1000 Router console:

  ```
  %EVENTLIB-3-TIMEHOG: F0: cpp_sp:  undefined: 30160ms,
  Traceback=1#ad497e64d353fac0e9ed1351f534cf6f   evlib:F3B0000+D120 evlib:F3B0000+A838
  cpp_common_os:F8E8000+10E2C cpp_common_os:F8E8000+10EDC evlib:F3B0000+DB60
  ```

  When 1K Prefixes with 5 traffic class each prefix is configured. The traceback could appear in the below mentioned scenarios:

  MC is already configured for 5K TCs with mode monitor both with traffic turned on and BR is reloaded with BR configs

  With MC is already configured for 5K TCs with mode monitor both with traffic turned on and issuing "**clear oer master ***" on the MC.

  With MC is already configured for 5K TCs with mode monitor both with traffic turned on and the best utilization value is moved from one link to another.

  Workaround: None

- CSCte50863

  An fman_fp core is generated when the Template ACL feature is disabled or enabled several times with 4k PPP sessions with per-user ACLs.

  This condition has been observed, when bringing up 4000 PPP Sessions terminated on PTA with per-user ACLs. With the template ACL feature enabled, only a few templates are created. Disable the template ACL feature and since there are only 4000 PPP Sessions, TCAM exhaustion by this action is not expected. Enable the template ACL feature again. Repeat until an fman_fp core is generated (usually seen within 10 iterations).

  Workaround: Is to tear down PPP Sessions before disabling and enabling the Template ACL feature.

- CSCtf06872

  Kernel crash may occur with GETVPN configuration (with 1 GDOI Group and 3 VRF's).

  This condition are seen with overnight traffic and the kernel crash may occur within a GETVPN Topology.

  Workaround: None

- CSCtf08810

  Multicast traffic loss observed in broadband environment.

  This condition happens after RP switchover, multicast traffic takes longer to converge.

  Workaround: None

- CSCtf16429

  Stale object has been seen on RP2 switchover with Route and MPLS flaps.

  Workaround: None

- CSCtf23385

  When PTA is configured for 32k PPPoEoA or 16k PPPoEoA AutoVC with the following kind of configuration:

```
interface atm 2/0/0.65000 multipoint
range pvc 1/32  1/4033
pvc-in-range 1/32
!
pvc-in-range 1/33
:
:  so on 4000 pvc-in-ranges
```

  Then when the PTA is unconfigured in the following sequence:

  1. First unconfigure all pvc-in-range
  2. then unconfigure range pvc
  3. unconfigure interface

  And reconfigured, it is found that all autovcs on the standby RP do not get created.

  The condition is caused due to specific order of unconfig as mentioned above.

  Workaround: Do not unconfigure the the above mentioned sequence. Unconfigure the interface only, then this issue is not seen.

- CSCtf43664

  Ucode crash on loading EoMPLS configuration on a Cisco ASR 1000 Router.

  This condition happens after starting up L2TPv3 while trying to copy EoMPLS configurations on the same interfaces.

  Workaround: None

- CSCtf57963

  On a Cisco ASR 1000 Router VRF with VRFx inspect vrf-default are added.

  This condtion may occur when the above option gets **enabled** as soon as the CLI “parameter-map type inspect global” is added with ZB Firewall.

  Workaround: None

- CSCtf81635

  Trace back warnings are observed in the log.

  This has been observed when changing the ACL configuration used by a large number of PPPoE Sessions while some of them are connecting or disconnecting.

Workaround: None

- CSCtf97660

  In an ASR 1000 Router configured for CUBE(SP Edition), a SIP session will sometimes terminate with a 503 error message. The PDLOG will indicate a “Socket Write Error”.

  This only happens when TCP is being used as the transport for SIP signaling and a media IP address was reconfigured to be used for a Signaling address without reloading.

  Workaround: Is to avoid re-using a media IP address for signaling or if required, save the configuration and reload after making the configuration change.

- CSCtf98979

  The following error message appears when stale object are seen after RP switchover:

```
6RU_BR2#sh platform software object-manager fp active stale-object
Object identifier: 2085
Description: Route-map name OER_INTERNAL_RMAP
Status: Done
Object identifier: 2090
Description: Feat 6, CG 1, rtmap name OER_INTERNAL_RMAP
Status: Done
```

  This condition are seen with dynamic route maps enabled and PFR setup. The switch over is done on the active BR and the stale object is seen.

  Workaround: None

- CSCtg01020

  IPSec tunnel fails (Phase 2) to establish between two ASR 1000 Routers when site-to-site VPN is configured due to invalid SPI.

  Workaround: The IPSec tunnel may come up after issuing a **reload**.

- CSCtg32407

  The RP may crash while unconfiguring ATM multipoint interfaces when configured with a different bba groups that has different session limits after bringing up the pppoeoa sessions.

  This instance may occur when an ASR 1000 Router has ATM Multipoint interfaces configured with different BBA Groups and the session limits are different.

  Workaround: Is to disable the pppoe config under interface level and then unconfigure the bba group.

- CSCtg33275

  A Cisco ASR 1000 plogd crashes when reloading Cisco IOS XE 2.6.0 Release when using 6RU with dual RP2.

  The following has been observed on the console:

```
core file “MCP-6RU-2_RP_0_plogd_25197.core.gz” is generated during RP0 reload.
```

  Workaround: There is no known workaround.

- 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.

- CSCtg53599

  The %COMMON_FIB-3-FIBIDBINCONS2 error has been logged on the standby RP after sessions are established.

  The condition has been seen when ASR1006 with dual RP1 and FP10 installed.

  The following error has been logged on the Standby RP multiple times after bringing up 10 PPPoEoA sessions with Model F QoS:

  ```
  *Apr 29 17:08:42.792: %COMMON_FIB-3-FIBIDBINCONS2: An internal software error
  occurred. Virtual-Access2.1 linked to wrong idb Virtual-Access2.1
  ```

  Workaround: None

- CSCtg59328

  When IPCP renegotiates for an existing PPPoE session, the new IPv4 address does not get synced up with the standby.

  This instance may occur when IPCP renegotiates for an existing PPPoE session, the new IPv4 address does not get synced up with the standby.

  Workaround: None

- CSCtg68228

  MQC on ATM VC fails to sync up with RP Standby.

  This condition may occur when MQC has downloaded from RSIM to an ATM and the AutoVC fails to sync up with RP Standby.

  Workaround: None

- CSCtg88218

  When establishing 128 ISG IP session with L4R feature that has duration with frequency provisioned on FP40, ucode core is generated with the following traceback:

  ```
  6RU8_L4R_UT#show running-config | b ge
  *May 17 21:33:23.092: %CPPHA-3-FAULT: F1: cpp_ha:  CPP:0
  desc:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR(interrupt) class:OTHER sev:FATAL
  id:2121 cppstate:RUNNING res:UNKNOWN flags:0x7 cdmflags:0x0
  *May 17 21:33:23.092: %CPPHA-3-FAULTCRASH: F1: cpp_ha:  CPP 0 unresolved fault
  detected, initiating crash dump.
  *May 17 21:33:23.093: %CPPDRV-6-INTR: F1:
  /tmp/sw/fp/1/0/fpx86/mount/usr/cpp/bin/cpp_driver[6366]:  CPP10(0) Interrupt :  May 17
  16:33:23.086438: :INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 ner
  ```

  This condition has been observed when sending traffic to establishing 128 ISP IP sessions that have L4Redirect with non-zero duration and non-zero frequency.

  Workaround: None

- CSCth03545

  A memory leak has been seen on a Cisco ASR 1000 Router when the traffic is sent for a long period of time (6 to 7 hours).

This condition has been observed when 1500 bytes of traffic are sent for a long period of time (6 to 7 hours) then it results in a memory leak followed by router crash.

Workaround: None

- CSCth09005

  Active RP crashes under heavy call load and 220 CPS is configured with billing enabled.

  This instance may occur under heavy call load and 220 CPS is configured on the Active RP with billing enabled.

  Workaround: None

- CSCth15799

  When issuing a ping to multicast the process fails from one of the hosts while Multicast Group is configured.

  This may occur when GDOI CM is applied to 2 interfaces and there is no local-addr confgured.

  Workaround: Is to clear crypto gdoi on the GM.

- CSCth27728

  After SBC has been configured on an ASR 1000 and a SIP call is made the router crashes.

  The conditions has been observed 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 the cause of the crash. Removing this from the config should result in the same behavior and avoid the crash.

  Workaround: The customer has changed “edit del-prefix 1 add-prefix 64” to”edit del-prefix 0 add-prefix 64”. Instead of this they should just use “edit add-prefix 64”.

- CSCth29934

  When Primary SIP OIR on the insertion side was executed, the Protocol-up delay of primay core side IF has been observed.

  Workaround: remove a physical line in core-side. After that, insert SIP and then no shut the IF.

- CSCth30370

  Traffic drops running Cisco IOS XE 2.6 on the ASR 1000 Router with AAA QoS Policy Accounting feature configured.

  Traffic drops are observed while doing ISSU upgrade when running Cisco IOS XE 2.6 with AAA QoS Policy Accounting feature configured.

  Workaround: None

- CSCth34753

  CPP Crash when shutting down WCCP interface with the following error message displayed on the console:

  ```
  un  8 16:32:35.218 pst: %CPPHA-3-FAULT: F0: cpp_ha:  CPP:0
  desc:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR(interrupt) class:OTHER sev:FATAL
  id:2121 cppstate:RUNNING res:UNKNOWN flags:0x7 cdmflags:0x0
  ```

  This conditions has been observed when WCCP is enabled on ASR1002 and data traffic is being redirected to WAE.

  Workaround: Is to gracefully shutdown WCCP in the WAE first before shutting down the router WCCP interface.

  For example:

  ```
  WAE-91#show wccp status
  ```

```
WCCP version 2 is enabled and currently active

WAE-91#conf t
WAE-91(config)#no wccp version 2
WCCP clean shutdown initiated
Waiting for shutdown ok (1 seconds) . Press ^C to skip waiting
WCCP clean shutdown wait time expired
WAE-91(config)#end

WAE-91#show wccp status
WCCP is not enabled
WAE-91#
```

The router will stop redirecting traffic to WAE once wccp service is disconnected from WAE.

For example:

```
In WAN1-1002-R46#
Jun 18 13:49:15.310 pst: %WCCP-1-SERVICELOST: Service 61 lost on WCCP Client
10.111.46.10
Jun 18 13:49:15.310 pst: %WCCP-1-SERVICELOST: Service 62 lost on WCCP Client
10.111.46.10
WAN1-1002-R46#
```

- CSCth38187

  Traffic is loss with IPv6 Static Route function, the ASR 1000 Router failed after clearing FIB.

  This condition occurred while checking the IPv6 Static Route function, some traffic was loss within IPv6 Static Route entries after clearing FIB on the router.

  Workaround: None

- CSCth41121

  An ASR 1000 Router crashes 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 crash is that the renegotiation adds an extra stream to the call (a new m= line in the SDP) and the reINVITE is rejected.

  Workaround: None

- CSCth42453

  SIP endpoints with shared line appearance fail to receive incoming call properly after an ASR 1000 Router failover.

  This is a SBC (CUBE(SP Edition) problem running on an ASR 1000 platform.

  There is no impact to normal SIP endpoint services.

  Workaround: None

- CSCth48008

  An ASR 1000 ESP may crash due to traffic which is being encrypted.

  The exact conditions for this are not yet known. Fragmented GRE traffic which needs to be encrypted may be the trigger.

  Workaround: There is no known workaround at this time.

- CSCth49752

  EoMPLS remote link status is not shown in the show sub-interface output.

This condition has been when EoMPLS remote link status is not shown in the show interface output when xconnect has binded into the dot1q encapsulated nterface.

Workaround: None

- 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

Resolved Caveats—Cisco IOS XE Release 2.6.2

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.6.2

- CSCsc49958

  AAA Authentication falback method to enable password does not work properly if RADIUS server is unavailalble.

  When the RADIUS server is unavailable, enter any username but then the enable password as the user password.

  Workaround: None

- CSCsx45326

  This is an enhancement to remove the performance optimization achieved by the ddts# CSCef70161.

  This condition happens when the **neighbor <> as-override** command was giving problems. This happened when it was used in an ipv4 VRF without SoO configuration on the PE and higher weight configuration on a particular CE.

  Workaround: To get the best performance optimization achieved in ddts# CSCef70161, when **neighbor <> as-override** is configured in ipv4 VRF. Use the SoO feature to isolate specific peer out of update-group.

- 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:

  BGP is configured

  More than one equally-good route is available

BGP is configured to use less than the maximum available number of multipaths

Workaround: There is no workaround.

- CSCsy23839

  On Cisco ASR 1000 Router Series, CPU utilization of SIP (SPA Interface Processor) may be 100%.

  This symptom is observed with the following procedure:

  1. Open a terminal window for telnet to ASR 1000.
  2. Telnet to ASR 1000.
  3. Run the request platform software console attach x/x (login SIP IOS) command.
  4. Close the terminal window without exiting from SIP IOS.
  5. You can see that the ioscon process is not terminated and its CPU utilization is around 100% by the monitor platform software process command.

  Workaround: Resetting the SIP resolves the issue.

- CSCsz45263

  ISIS fails to come up due to the redundant 'clns mtu' is being added under the tunnel interface configuration.

  This symptom is seen, after reload of the router.

  Workaround: None

- CSCsz53438

  When ip header compression is configured on the ASR 1000 Router, but not on the corresponding router, an unexpected reload of the embedded systems processor may occur.

  This has been seen, when IPHC is configured on the ASR 1000 Router, but not on the router to which it is directly connected.

  Workaround: Is to **enable IPHC** on both routers.

- CSCsz60746

  A static route configured through an unnumbered interface which is in shutdown state will not show up in RIB even after the interface state is UP.

  This condition has seen seen when configuring a static route on a shut down interface having ip unnumbered configuration.

  Workaround: Is to remove and re-add the static route.

- CSCta11120

  When two servers are configured under a group; the first server in the group is inaccessible. At the time of the first request, the request failed over to the second server in the group. The first server in the group comes up; however, the router uses the second server to process the request instead of the first server.

  In addtion, when a single-connection is configured, switch uses only primary tacacs server for http authorization even though the primary server is down.

  This condition has been seen when two servers are configured under a group; the first server in the group is inaccessible At the time of first request, the request fail-over to second server in the group.

  - HTTP Authorization is configured for switch's GUI access
  - Multiple TACACS servers are configured with single-connection option
  - Primary Tacacs server is down

Workaround: Disable single-connection

- CSCta40318

  IOS or the IOSd may crash on a Cisco ASR 1000 Router.

  This condition has been observed when ISAKMP CAC (call admission control) is configured, the CAC limit is reached and **debug crypto isakmp** is **enabled**.

  Workaround: Is to **undebug crypto isakmp**.

- CSCtb58282

  When anASR 1000 is running Cisco IOS, the device may reload when **show tcp brief** is issued.

  This condition has been seen when the following has occurred:

  1. The “ip domain lookup” 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 (in the order of 70 characters, only).
  3. The port number of the foreign host needs to be 5 digits long.

  When the ip domain lookup is disabled, the problem could still happen if the host has a static entry configured via the “ip host” command.

  Workaround: Is to configure “no ip domain lookup”. Or, avoid using **show tcp brief** on the device.

- CSCtc62440

  On a Cisco ASR 1000 Router Series, the removal of sub-interfaces 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.

- CSCtd09817

  ISG L2 Connected DHCP session is terminated on renewal after vrf transfer.

  This condition has been seen when an ASR 1000 Router is configured as ISG for L2 connected subscriber session and vrf transfer is done without any change in dhcp class.

  Workaround: None

- CSCtd34056

  This enhancement request is to allow for **crypto pki crl ca size** to be saved in the ASR 1000 Router config and to not disappear after reload.

  Workaround: None

- CSCtd89923

  Webex SPA hard disk sectors are corrupted. This condition has been observed when SIP10 is configured with a Webex SPA running release 2.6.0 image that is Soft-OIR'ed. This configuration can potientially corrupt the sectors on the hard disk of the Webex SPA.

  Workaround: Is to shutdown the SPA before reloading the SIP10.

- CSCte08821

  When **sh l2tp session packets tunnel id** is issued on an ASR 1000 Router with wrong session id, the session id shows as a junk value.

  Workaround: None

- 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

  An unexpected reload may happen on the ASR 1000 Router Series. This has seen, when BGP VPNv4 is configured and a neighbor is flapping on the router.

  Workaround: None

- CSCte21062

  Session churn shows a slow memory leak which manifests during individual session teardown when the one sec accounting accuracy feature is **enabled**.

  This condition has been observed when, **subscriber accounting accuracy <VALUE>** is configured, background variables are allocated to support feature messaging. These variables are allocated a small amount of memory which is unfortunately not freed when the session is disconnected. This leads to a small memory leak averaging between 50-60 bytes per session disconnection.

  Workaround: Removal of configuration related to subscriber accounting accuracy.

  Example: **no subscriber accounting accuracy 1000**

- CSCte37344

  The following IOS console message is printed during an attempt to add a non-queueing class to the 2nd level of a 3-level hierarchy, within a QoS policy that is attached to one or more interfaces:

  At least one queueing feature needed for every class in the 2nd level policy with 3-level of hierarchy

  Subsequent operations, even policy-map removal, will cause failures.

  This condition happens when 3-level QoS policy-map is applied to one or more interfaces, when additional 2nd level classes are added (depending on the timing of events), even if the classes have queueing features, the user may see the following console message:

  At least one queueing feature needed for every class in the 2nd level policy with 3-level of hierarchy

  Once this message appears, subsequent attempts to modify or detach the policy will encounter errors and/or classification will not work correctly.

  Can be seen when running 12.2(33)XNF.

  Workaround: If the problem occurs, the FP/ESP must be rebooted.

  To avoid the problem, remove the QoS policy from all interfaces first, make the policy-map modifications, then re-attach the policy.

  Further Problem Description:

  The problem occurs because the class-add event **leaks-through** even though the class-add operation is not allowed. From this point forward, IOS and PD layers are out-of-sync, so there are even errors on policy-map detachment and removal.

- CSCte39643

  When PfR receives an EIGRP route change, the router may unexpectedly reload.

The symptom is observed with PfR and EIGRP configurations. It is observed some time after PfR receives an EIGRP route change, but before the previous EIGRP route is removed in the routing table, when PfR tries to recycle a previous EIGRP route.

Workaround: There is no workaround.

- CSCte49283

  Sometimes the LNS router sends an incorrect NAS-Port value.

  The symptom is observed when the LNS router sends a stop accounting-request to the RADIUS server.

  Workaround: There is no workaround.

- CSCte64750

  Slower PPPoE sessions bring up rate on the Cisco ASR 1000 Router.

  This condition was observed when L2TP HA and congestion control has been enabled.

  Workaround: None

- 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: None

- CSCte82351

  The BGP aspath encoding in snmp (bgp4PathAttrASPathSegment) is encoding all aspath information as 32bit. This is not compatible with RFC4273 which defines this oid.

  This condition may occur on all IOS versions.

  Workaround: None

- CSCte84710

  When IPv6 Unicast is enabled on an ASR 1000 Router the following error message is displayed on the console:

  error message flag_icmp_error_gen type 1 and code 0 popup

  Workaround: None

- CSCte87294

  The following L2TP related error with traceback might show up on the Standby RP:

```
L2TP-3-ILLEGAL: _____:________: ERROR: Unable to reserve session ID 2047
Traceback summary example:
0x11305a7 is in errmsg
0x1f1c056 is in l2tp_errmsg_internal
0x1f1c1e8 is in l2tp_errmsg
0x1f1c33f is in l2tp_error_traceback
0x35ab131 is in l2tp_ha_create_session
0x35b1791 is in l2tp_ha_process_ICRQ_chkpt
0x35b0e90 is in l2tp_ha_process_proto_session_chkpt
0x35b0749 is in l2tp_cpf_process_message
```

```
0x35b0648 is in l2tp_chkpt_q_handler
0x35ae86f is in l2tp_ha_l2tp_msg_handler
0x1f5215e is in l2tp_ha_l2tp_msg_handler_os
0x1f25e73 is in l2tp_mgr_process
```

The session on the active will not be present on the standby.

This only happens when the tunnel goes down and a session id belonging to the tunnel gets reused on the active.

Workaround: Is to Reboot the standby, after bulk sync the Standby RP will match the Active RP.

- CSCte95275

  When an ASR 1000 Router is out of free memory, some FMI codes are trying to free up memory out of the NULL chunk that has never been created.

  This condition is observed when the ASR 1000 Router is out of free memory.

  Workaround: None

- CSCte97814

  On an ASR 1000 Router with BGP enabled, a small fixed size chunk memory leak is observed during boot-up. To be exact, it is observed just after config bulk-sync in redundant RP setup.

  This symptom is observed on Cisco ASR 1000 Series Routers with a redundant RP setup and BGP enabled.

  Workaround: There is no workaround.

- CSCtf01618

  A Cisco ASR 1000 Router may unexpectedly reload due to SegV error.

  This condition has been observed, when the ASR 1000 Router must be running 12.2(33)XND1 or later XND or 12.2(33)XNE or even later 12.2(33)XN releases and DMVPN is configured with Tunnel Protection.

  Workaround: Remove Tunnel Protection.

- CSCtf04257

  On an 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. When destination of VC is changed from original to something else and then changed back to original.

  Workaround: None.

- CSCtf13343

  Command authorization for commands involving a 4-byte ASN fails. Command accounting for these commands will record an incorrect ASN or ip address.

  The following commands are impacted:

  Global configuration mode:

  router bgp x.y

  BGP configuration submode:

  neighbor <address> remote-as x.y

  ip vrf <vrf name> submode:

route-target <ip address>:X

route-target x.y:z

route-target y:z

If you turn on the relevant AAA debugs, you will see some arguments appear multiple times in a given authorization or accounting request, and others not appear at all.

This problem is seen whenever command authorization and/or command accounting is configured for any of the following commands:

Global configuration mode:

router bgp x.y

BGP configuration submode:

neighbor <address> remote-as x.y

ip vrf <vrf name> submode:

route-target <ip address>:X

route-target x.y:z

route-target y:z

A typical affected configuration in 12.0 and earlier would say:

aaa new-model

aaa authorization commands 15 default tacacs+

A typical affected configuration in 12.0T and later would say:

aaa new-model

aaa authorization commands 15 default group tacacs+

Workaround: You may be able to permit authorization of affected commands by allowing changing you tacacs+ server configuration to permit commands which include repeated arguments.

There is no workaround for the incorrect accounting records.

Further Problem Description: IOS releases not including 4-byte ASN support see a more limited form of this problem where only the first and last byte of the ipv4 address are sent to the AAA server. On such releases, the ASNs are sent as normal.

In Cisco IOS Release 15.0 and later, only the route-target command is tracked by this CSCtf13343. You need to have CSCtg42163 and CSCtg42088 integrated as well in order to get the fix for router bgp x.y and neighbor <address> remote-as x.y respectively.

- CSCtf13704

  Memory leaks are seen when Graceful Restart is configured on an ASR 1000 with BGP sessions processing.

  The following error message can appear during Graceful Restart:

  %BGP-3-NEGCOUNTER

  The symptom is observed with non-NSF Graceful Restart on releases with the fix for CSCtd99802.

  Workaround: There is no workaround.

- CSCtf15982

  While large number of DHCP sessions are coming up, the router may crash due to corrupted chunk header.

This issue happened while large number of unauthenticated sessions were coming up but it may also happen for authenticated sessions. There's no clear condition as to why this has happened.

Workaround: There is no known workaround at this time.

- CSCtf23727

  On a dual-RP PE router where a BGP CE peer is connected via a PPP link and the CE peer is also configured for NSR (**neighbor ha-mode sso** command), forwarding for prefixes learned from the CE router may fail after an RP switchover. After the switchover, the affected routes appear in the BGP table without a bestpath and the reason **nexthop inaccessible** listed.

  The problem can be seen when all of the following conditions are true:

  - The PE router is dual-RP
  - The PE router is configured for SSO redundancy mode and is operating in hot standby mode
  - The PE is connected to a CE router over an PPP link
  - On the PE router, the CE neighbor is configured for BGP NSR
  - BGP learns prefixes from the CE and the nexthop addresss for those prefixes are via PPP
  - An RP switchover is performed

  Workaround: **Shut** and **unshut** the PPP link to the affected CE or **disable** nexthop address tracking (**no bgp nexthop trigger enable**) for VPNv4 and re-enable 1-2 minutes later.

- CSCtf27187

  Traffic stops after initiating SPA OIR.

  This symptom is observed only when initiating SPA OIR.

  Workaround: Is to do a SIP OIR, the traffic should resume.

- CSCtf28793

  When an ASR 1000 has the following configuration in BGP:

  aggregate-address ***ip addresss*** summary-only advertise-map

  route-map name suppress-map ***route-map name***

  Additional configuration are observed:

  - Routes matching the suppress-map are not suppressed.
  - The aggregate address is advertised.

  The above condition are seen with a **reload** or after a hard **clearing** of BGP Peers. Both the advertise-map and suppress-map must be configured.

  Workaround: Is to reconfigure the aggregate command, or use an aggregate command without the advertise-map/suppress-map combination.

- CSCtf29685

  LNS Router crashed when sending accounting stop request.

  This condition is observed when PPPoE setup is configured with LAC and LNS. In addition, when LNS downloads the account the process is stopped with failures when configurations from AAA server with template type are initiated.

  Workaround: None

- CSCtf33539

When an ASR 1000 supporting L2TP High Availability and managing a large number of L2TP tunnels as a LAC or an LNS, may spontaneously reload in very rare circumstances, shortly after a stateful switchover or SSO, with a stack trace similar to the following example:

```
0x12f5ce4c is in l2tp_ha_sfo_resync_done
0x12f5ce24 is in l2tp_ha_sfo_resync_done
0x1215bfb0 is in
l2tp_ha_resync_receive_control_packet_os
0x12135920 is in l2tp_manage_ctrl_conn_for_pak
0x121369f8 is in l2tp_process_control_packets
0x1212fc88 is in l2tp_mgr_process_control_packets
0x1212fe0c is in l2tp_mgr_process
```

This condition has been observed when ASR 1000 supports L2TP High Availability and managing a large number of L2TP tunnels as a LAC or an LNS,

Workaround: There is no workaround.

- CSCtf36152

  When ASR(LAC) receives StopCCN from LNS due to the lack of resources (L2TP session limit), the ASR (LAC) returns ZLB with bad sequence number.

  In this case, the correct Ns/Nr of ZLB should be Ns=1/Nr=1.

  Workaround: None

- CSCtf47795

  An ASR 1000 Router may crash when **show ip bgp neighbor** command is executed.

  Workaround: None

- CSCtf50075

  A traffic blackhole can occur on the Cisco ASR 1000 Router Series.

  The symptom is observed following **shut/unshut/shut** during redundant forwarding on an interface.

  Workaround: There is no workaround.

- CSCtf51834

  After a stateful switchover (SSO) on an IOS router supporting L2TP HA, the counter showing the number of L2TP sessions which were destroyed because they were not completely established at the time of the SSO, may be incorrect.

  This counter is visible with the command show l2tp redundancy detail in the section Sessions destroyed during resync phase.

  For example, the sessions destroyed during resync phase:

  ```
  Poisoned:         0
  Unestablished:    10    -- This value may be incorrect
  Tunnel in resync: 0
  ```

  After a stateful switchover (SSO) on an IOS router supporting L2TP HA.

  Workaround: No workaround.

- CSCtf65536

  ESP can crash while performing SIP calls using Cube-SP function.

  This symptom is observed when hairpinned SIP calls are present, but it is timing related, so it doesn't occur in all cases.

  Workaround: There is no workaround.

- CSCtf66633

  A Floating static route with the **permanent** keyword may not get installed into the routing table when the primary route goes down.

  Workaround: None

- CSCtf69391

  Output drops on an interface incrementing apparently due to ISG with session drops.

  This condition may happen when Low traffic has been seen on the interface. This appears to be actual packet drops from trafficon an interface.

  Workaround: None

- CSCtf70312

  When POS PA OIR and HA (using the Active RP crashed) simultaneously resulted in SIP crash.

  SPA is OIRed and active-RP is forced crash(using "test crash" cli)simultaneously.

  This resulted in the following message seen on new active RP due to SIP reset:

  ```
  %PMAN-3-PROCHOLDDOWN: SIP0: pman.sh:  The process mcpcc-lc-ms has been helddown (rc
  134)
  ```

  Workaround: None

  Further Problem Description: The following trace for the SIP is displayed on the console:

  ```
  <3478133836,4037269920>: %ASR1000_SIP_SPA-3-IPCPORT: SIP0/2: Failed to open
  IPC port 'IPC Master:
  Slot 0/2 ICP', error session in use
  ```

  Reproducibility:

  Is very low, unless there is no delay between SPA OIR and RP is forced to crash. This defect cannot be reproducible.

  Impact: The SIP is crashed and reloaded with “process mcpcc-lc-ms has been helddown” message.

- CSCtf70851

  Input/Output Rate freezes and doesn't get updated. This symptom is observed if the interface is **shut** with the traffic running, the input/output rate gets stuck and doesn't go back to 0.

  Workaround: Giving **no shut** on the interface restarts the input/output rate.

- CSCtf71575

  CE to CE ping failed over when EoMPLS is configured on a Vlan interface.

  This condition has been observed when CE to CE ping failed with EoMPLS configured on a native Vlan interface.

  Workaround: None

- CSCtf71998

  The follow tracebacks are seen while PPTP sessions are being processed:

  ```
  Mar  9 06:32:40 coltel-gw 231109: Mar  9 03:32:49.413: %SW_MGR-3-CM_ERROR: Connection
  Manager Error - provision segment failed [SSS:PPTP:17175151] - add to database fail.
  Mar  9 06:32:40 coltel-gw 231110: -Traceback= 4B5E50 4B6DDC 4B7504 12D3D34 12D3E84
  2555B20 2555BF8 12D135C 27A8DA4 27A8E54 12D1E80 12D2014 12C2C14 27A8DA4 27A8E54
  12C38A8
  ```

  This condition are observed on LNS when VPDN group with PPTP has been configured.

  Workaround: None

Further Problem Description: Tracebacks are thrown every few seconds on LNS with PPTP configurations, while sessions are coming up.

- CSCtf75446

  The Cisco ASR 1000 Router console may freeze up in unconfiguring atm subinterface.

  Workaround: None

- CSCtf78196

  Although tunnel interface has alternative path to an OSPF neighbor, when the primary interface goes down, the tunnel interface goes down for a moment.

  The symptom occurs when a tunnel tracks an MTU from higher value to a lower value on the outgoing interface. (It is seen on many images)

  Workaround: Statically configure "**ipv6 mtu <mtu>**" on tunnel interfaces.

- CSCtf79163

  Asymmetric carrier delay does not work on an ASR 1000 Router.

  This conditon has been observed when asymmetric carrier delay is configured on the router.

  Workaround: Is to use symmetric carrier delay.

- CSCtf80105

  When basic SIP-SIP calls are placed using automation scripts, calls start failing due to UDP socket connection error.

  The symptom is observed when the router is configured with a dial peer and with SNMP. A dial peer is most likely required to reproduce the issue, but it is possible that a different UDP protocol other than SNMP could also cause the symptom. Once a call failure occurs, all the calls placed later will fail with a UDP socket connection error.

  Workaround: Use the following steps:

  1. Under sip-ua, configure **connection-reuse** (which is a hidden command).
  2. Configure the use of TCP.

- CSCtf80843

  On an ASR 1000 Router tracebacks are seen when PBHK do not have a port mapping for an active connection.

  This instance would only occur after clearing IP sessions on the router where active PBHK port mappings exists.

  Workaround: None

- CSCtf82883

  When clearing a VRF route, there is a traffic drop on other VRF routes.

  The symptom is observed with an L3 VPN configuration.

  Workaround: There is no workaround.

  Further Problem Description: Some LTE broker distribution is leaked to other VRFs.

- CSCtf83092

  Standby resets continuously while ISSU upgrade from a non-componenterized IOS image to a componenterized IOS image.

  The issue is seen with an MPLS VC configuration.

Workaround: There is no workaround.

- CSCtf84237

  An Cisco ASR 1000 Router may reload with the following crash decoded tracebacks:.

  In this example, the summary traceback has been observed:

```
0x123d7e24 is in vpdn_apply_vpdn_template_pptp
0x1239c100 is in l2x_vpdn_template_find
0x123d81dc is in vpdn_apply_l2x_group_config
0x123cfedc is in vpdn_mgr_call_initiate_connection
0x123cce68 is in vpdn_mgr_event
0x123ce974 is in vpdn_mgr_process_client_connect
0x123cf248 is in vpdn_mgr_process_message
0x123cf368 is in vpdn_call_manager
```

  This condition may happen when an invalid tunnel-type VSA is configured as shown in this example:

  vsa cisco generic 1 string **vpdn:tunnel-type=l2tp_bad**

  Workaround: Is to configure a correct tunnel-type VSA in Radius.

- CSCtf86998

  In a GETVPN ASR 1000 Router Series deployment, packets on one of the ASR GM router interfaces are not encrypted.

  This symptom is observed when GM1 is in passive mode.

  Workaround: There is no workaround.

- CSCtf90157

  When an ASR 1000 selects link local address instead of global unicast address of unnumbered loopback interface to send ICMPv6, the time exceeds packet over Virtual Access over the interface.

  Workaround: There is no workaround.

- CSCtf92423

  After switchover on an ASR 1000 Router the Peer routes are learned from PPP and are not in RIB/CEF tables.

  This symptom is observed when Switchover with PPP are learned on each of routes.

  Workaround: None

- CSCtf93465

  In a CUBE(SP Edition) ASR 1000 Router, the following message is seen when trying to enter SBC config mode:

  SBC: Internal error - SBC configuration cannot be processed.

  This condition sometimes happens after unconfiguring SBC.

  Workaround: The workaround is to do a reload.

- CSCtf95905

  An ASR 1000 Router may crash in the BGP HA SSO process. The following error message is shown when the standby RP is booted:

```
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk <hex-addr>  data
 <hex-addr>  chunkmagic <hex-addr>  chunk_freemagic <hex-addr> -Process= “BGP HA
 SSO”
```

  The symptom is observed with the following conditions:

- The router is configured for SSO redundancy mode.
- BGP is configured.
- Some BGP peers have NSR configured (using the **neighbor ha-mode sso** command) and NSR is active for those peers.
- The standby RP is loaded and progresses to hot standby state after NSR sessions are already established on the active RP.

Workaround: Is to configure peers intended to be **enabled** for NSR for passive open only (using the **neighbor transport connection-mode passive** command) and then **enable** NSR on the BGP peers after the router has already reached hot standby state.

- CSCtf98758

  Standby RP crashes after replacing the basic configuration of the router with an au3-e3 configuration.

  This symptom is observed after initiating the following steps:

  1. Configure the router with back-to-back SDH link for full AU3-E3 configurations with SPA-1XCHOC12/DS0.
  2. Save the running configuration using **copy run bootflash:au3-e3.conf**
  3. Reload the router with config register set to 0x2142. This will get the router running configuration to the basic default configuration.
  4. After the router is up with redundancy setup and basic default configuration, execute the config replace command with the target config that was saved in step 1. {Config replace bootflash:au3-e3.con}

  Workaround: There is no workaround.

- CSCtf98802

  Config replace command when executed in a particular way causes the router to malfunction.

  This symptom is observed after the following steps:

  1. When we try to remove channelized configuration using config replace command, it will ask for the confirmation of the same as below:

  Unprovision clear channel interface ?[confirm]

  2. If we put any character other than 'y' or 'n' it will not remove the channel configuration for that particular path.
  3. Now, if I try to remove these channels that were not cleared before manually, the system is behaves improperly:

```
Router(config-controller)#au-3 1
%ERROR: Standby doesn't support this command                          ^
% Invalid input detected at '^' marker.

Router(config-controller)#
As you see above system is not allowing to enter into the controller configuration
mode and resulting into "%ERROR: Standby doesn't support this command" message.
```

  Workaround: By this point of time only after reload of the router, the situation comes under control and then only we can alter the controller configurations.

- CSCtg04289

  After all the detached adjacancies are changed the **congestion sip buffer-tuning** and **congestion sip pool-size InbPoolSize 8000 CLI** command an ASR 1000 Router may reload.

This symptom is observed after viewing the IPS trace which indicates that there is a bug in the CLI code. The CLI deactivates the SIP TM entity before changing the buffer pool size, but then afterwards does not reactivate the SIP TM entity.

Workaround: None

- CSCtg06730

  When following parameters of BASEROOT package set by MGC, that overwrites T-MAX configuration on DBE:

  root/normalMGCExecutionTime

  root/MGCProvisionalResponseTimerValue

  This condition is observed when bringing up H.248 session and MGC set the parameters by Modify message.

  Workaround: None

- CSCtg11491

  System may encounter CPUHOG and an error 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 thru CLI : clear radius-proxy client <ip
  addr>
  ```

  This symptom is observed on a Cisco ASR 1000 Series Router when functions as an Inteligent Service Gateway (ISG) Radius Proxy, when thousands of sessions were established.

  Workaround: There is no workaround.

- CSCtg12139

  On an ASR1006 running IOS 12.2(33)XNF with SPA-2XCT3/DS0 card in slot 0/3SPA-2XCT3/DS0 is configured sends an alarm that the **DS3 Port Admin Down**.

  This symptom is observed when an ASR1006 running IOS 12.2(33)XNF with SPA-2XCT3/DS0 card in slot 0/3SPA-2XCT3/DS0 is configured after one of the T1s on DS3 0/3/0 changes state, the **DS3 Port Admin Down** alarm for DS3 0/3/1 (the other DS3 on that card) is clearing and being re-inserted.

  Workaround: Is to ignore the alarms as it not affecting any functionality.

- CSCtg12975

  Memory leaks are seen due to the Allocation PC (**L2TP mgmt daemo)** and Name (**L2X GRP CLASS NAME)** in **show memory debug leaks** output.

  The Memory Leaks occurs when vpdn group config is removed while l2tp tunnel is still up.

  Workaround: Is to take down tunnel before removing vpdn group from config.

- CSCtg13217

  ICMP Fragmentation required (type 3, code 4) and Host Unreachable Administratively (type 3, code 13) is not sent back if packets are hitting MTU checking, or ACL deny on Egress interface.

  This condition is observed when an ASR 1000 Platform is running IOS 12.2(33)XNE.

  Workaround: There is no workaround.

- CSCtg13790

  An ASR 1000 Router may crash while placing a call with **no call-route p-called-party-id**.

This instance may occur as shown in the following example:

1. sipp--->CUBE (SP)--->-sipp
2. SIP to SIP call
3. Placed a call with INVITE sip:uJVvp1GE4YDaWiEVqCLE7Ql9Y1bph7xF@9.45.39.1:5060 SIP/2.0
4. and uJVvp1GE4YDaWiEVqCLE7Ql9Y1bph7xF is in the Contact header of REGISTER request
5. Validation fails since **call-route p-called-party-id** is disabled
6. CUBE(SP Edition) crashes due to validation failure since **call-route p-called-party-id** is disabled.

Workaround: None

- CSCtg16498

  LNS VPDN message is incorrect when receiving CDN from LAC as follows:

  ```
  %VPDN-4-SESSIONERROR: L2TP LNS R102 unable to terminate user cisco@cisco.com; Result
  1, Error 0, No disconnect reason given
  ```

  It should start with "%VPDN-4-SESSIONERROR: L2TP LAC".

  This occurs when receiving CDN's result code is "1" and the following is configured on the router:

  vpdn logging is enabled

  Workaround: There is no workaround.

- CSCtg16516

  In a CUBE(SP Edition) ASR 1000 system, the bandwidth limits are reported in statistics even though tman/pol is OFF. This contion occurs when tman/sdr or tman/pdr is set.

  Workaround: Don not set tman/sdr or tman/pdr when tman/pol is OFF.

- CSCtg16544

  In a CUBE(SP Edition) ASR1000 system, the bandwidth limit for Side B is being reported for Side A, even though no bandwidth limit is set for sideA. This condition occurs when a bandwidth limit is configured for Side B, but not for Side A.

  Workaround: Is to configure bandwidth limits for both sides.

- CSCtg18261

  The BR fails to learn an application which is configured to learn traffic for a flow with dscp ef set.

  This condition is observed when the BR fails to learn an application which is configured to learn traffic for a flow with dscp ef set. **show ip cache v flow** shows that the flows are seen and traffic is going through but the application does not get learned. There are 2 applications configured at same time, one for tcp and 2nd for dscp ef. The 1st one gets learnt but not the second one.

  Workaround: None

- CSCtg18726

  When using an ASR 1000 Router the route may fail to originate network (type-2) LSA and therefore not to install routes to the routing table.

  This condition are seen in design with backup interface, when the following has occurred:

  - backup interface has same IP address like primary
  - OSPF network type is broadcast

  - both, primary and backup interfaces are configured to act as DR

  Workaround: Use p2p network type. Do not configure pair of primary/backup interfaces to act as DR.

  Further Problem Description: This is day-1 issue, all IOS releases without fix are affected (if configuration matches conditions, note, it's rare configuration).

- CSCtg21602

  In this example the following message is displayed on the Active RP Console:

```
%CPPOSLIB-3-ERROR_NOTIFY: F1: cpp_cp:  cpp_cp encountered an error -Traceback=
1#ed4b69bc77a25ff35c522388cbb72a96   errmsg:D94E000+2160 cpp_common_os:E0A4000+B920
cpp_common_os:E0A4000+19148 cpp_exmem_mgr:ED1E000+895C cpp_exmem_mgr:ED1E000+9080
cpp_common_os:E0A4000+163D0 cpp_rrm_local_api_lib:EFDF000+3150
cpp_rrm_svr_lib:F004000+53F0 cpp_rrm_svr_lib:F004000+76CC cpp_rrm_svr_lib:F004000+80A4
cpp_rrm_svr_lib:F004000+9810 cpp_dmap:E954000+15264 cpp_dmap:E954000+21BF4
cpp_common_os:E0A4000+
```

  This message is displayed right after un-configuring sbc by entering command:

  no sbc global dbe

  Workaround: None

- CSCtg23952

  Gratuitous ARPs are sent on all interfaces when performing a copy tftp operation.

  This condition happens when performing a copy tftp operation.

  Workaround: None

- CSCtg25056

  OSPF IEFT GR recovery aborts on restarting an ASR 1000 Router when ip address of OSPF enabled interface is also assigned on another interface of the same router which is admin down.

  Workaround: Remove duplicate ip addresses from admin down interfaces.

- CSCtg26760

  On an ASR 1000 Platform, WCCP redirection does not work after a reload, or following a change in the redirect ACL.

  The syslogs show a message similar to the following:

  %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image: Batch type 6 ID 318 download to CPP failed

  Workaround: The only known workaround is to reboot the router.

- CSCtg30995

  Delay of RP switchover associated with NV_BLOCK_INITFAIL message appearing on standby-turned-active RP console. When the manual switchover command, **redundancy force-switchover** and a filesystem command like **copy running-config startup-config** is issued from different consoles of active RP almost at the same time, such a problem may occur.

  Workaround: Avoid issuing any filesystem access command simultaneously with the manual RP switchover command. Should the above problem occur, please execute the same filesystem command, say, **copy running-config startup-config** from the standby-turned-active console.

- CSCtg32004

After applying QoS Model C / D2 configuration on PTA and on issuing the cli **show platform hardware cpp active infrastructure bqs status** the output of **" # of Active Schedules"** value is less than the expected one.

This condition is observed ASR 1000 Router with RP2 Processor configured with Model C / Model D2.

Workaround: None

- CSCtg32647

  Crypto tunnel fail to come up and the following message is displayed on the console:

  ```
  %CRYPTO-3-IKMP_QUERY_KEY: Querying key pair failed.
  ```

  This condition is observed when running IOS XE 2.6.0. Other releases may be affected.

  Workaround: Downgrade to IOS XE 2.4.1. Other versions might work as well.

  Further Problem Description: The issue happens while validating the peer certificate.

- CSCtg35230

  VPDN sessions are created when SCCRQ and SCCRP have different ip addresses on an ASR 1000 Router.

  This condition has been observed once the ip address is downloaded from the AAA server, the change to the IP address on LNS2 while creating two VPDN sessions.

  Workaround: None

- CSCtg37082

  Following warning messages are seen on active RP upgrade (ISSU) and switchover after upgrading to Release IOS XE 2.6.1 from 2.3.0e:

  ```
  %IMRP-3-IMRP_MSG_CANNOT_RELAY: R1/0: imand:  IMRP Peer ios_rp_iosd_slot_1:
  cannot relay message to SPA 15/15
  %IOSD_IMCC_CAPI-3-MSGDISPATCH: SIP2/1: Unable to dispatch received TDL
  ```

  After ISSU upgrading the active RP to IOS XE Release 2.6.1 from 2.3.0e, when RP switchover is initiated this warning will be seen on the newly active RP.

  The warning messages do not affect the general working of the SPA during ISSU when the VLAN Tunnel mode feature is not used.

  Workaround: None

- CSCtg38018

  An ASR 1000 Router could hang when static session is provisioned on the box upon switchover.

  The following conditions has been observed upon switchover:

  1. IP static session is provisioned
  2. IP session is not HA aware
  3. Switch-over is performaced

  Workaround: Deprovisioned static session before switch-over, after standby takes over, and become active unit. Reprovision static session.

- CSCtg40901

  An ASR 1000 Router crash is seen while authenticating with TACACS.

  The symptom is observed if the TACACS server does not respond.

  Workaround: Is to use multiple connections.

Alternate Workaround: Is to configure a dummy TACACS server.

- CSCtg42998

  An IOS XE Router supporting L2TP HA and acting as a LAC, may fail to effectively clear VPDN sessions which were cleared by the Client or LNS device just at the time when a stateful switchover is occurring.

  This condition may happen when L2TP HA Route Processor switchover has occurred. In addition this problem may surface around 2 seconds or less, after a stateful switchover.

  Workaround: An idle timer may be configured on the LAC.

  The following commands should be configure on the relevant Virtual-Template:

  interface

  ppp timeout idle

  ip idle-group access-list in|out

  or

  The sessions can be cleared manually by an operator.

- CSCtg44097

  Connect-Info 77 attribute is sent twice in a Pre-Auth Access-Request.

  Workaround: None

- CSCtg46605

  Due to caching issues the memory is cached and freed as required, this gives deceptive Free memory values when monitoring the ASR 1000 Router. The router had been changed to use the committed memory for monitoring the memory utilization, but users ar not able to monitor the committed memory via SNMP.

  This condition has been observed when monitoring the memory utilization on an ASR 1000 Router Platform.

  Workaround: Is to use the CLI **show platform software status control-processor brief** to retrieve the committed memory.

- CSCtg50288

  Standby RP crashes when configuring NAT Pool.

  This condition are observed when the Standby RP crashes, while processing the following steps, below:

```
ASR-2RU(config)#ip nat pool pool-60 66.0.0.0 66.0.255.255 prefix-length 16
ASR-2RU(config)#ip nat pool pool-60 66.0.0.0 66.255.255.255 prefix-length 8
%Error, pool size should be maximum 19 bits long
ASR-2RU(config)#ip nat pool pool-60 66.0.0.0 66.0.255.255 prefix-length 16
%Unable to synchronize pool with standby RP
ASR-2RU(config)#
*Apr 28 16:23:14.318 IST: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_NOT_PRESENT)
*Apr 28 16:23:14.318 IST: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_DOWN)
*Apr 28 16:23:14.318 IST: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
*Apr 28 16:23:14.386 IST: %IPNAT_HA-3-TRANSMIT: Unable to send via IPC
IPNAT_ADDRPOOL_MSG pool  pool-60 id 7; retry queue flush
-Traceback= 1#cc462b2a175cd9784a73925c8c37beb5  :10000000+C49434 :10000000+C497B8
:10000000+2C77E38 :10000000+157B8E8 :10000000+157BEEC :10000000+1551070
:10000000+BB4DEC :10000000+BBB688 :10000000+2B07D90 :10000000+BC989C
```

```
*Apr 28 16:23:21.604 IST: %RF-5-RF_RELOAD: Peer reload. Reason: EHSA standby down
*Apr 28 16:24:06.115 IST: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby
insertion (raw-event=PEER_FOUND(4))
```

Workaround: None

- CSCtg50351

  Two RADIUS access-request messages are sent upon receiving DHCPv6 SOLICIT message.

  This can occur when the ASR1000 has been configured as a BRAS Router with "i**pv6 nd prefix framed-ipv6-prefix**" configured.

  Workaround: There is no workaround, unless **"no ipv6 nd prefix framed-ipv6-prefix"** can be configured.

- CSCtg50359

  Asymmetric carrier delay values are not updated or present in running-config with in these 2 examples:

  1. - set carrier-delay msec 0

     - set carrier-delay up/down msec <any>

     --> uses the configured msec timer but running-config still shows **carrier-delay msec 0**.

     --> when symmetric carrier delay already configured, the configuring of asymmetric delay need be blocked, i.e first the symmetric carrier delay need to unconfigured before configuring any asymmetric values.

  2. - set **no carrier-delay msec 0**

     - set **carrier-delay up msec 1**

     - set **carrier-delay down msec 0**

     --> the down timer is not updated and not visible in the running-config

  This conditon will be visible from IOS XE 2.5 (12.2(33) XNE releases) and onwards.

  Workaround: None

- CSCtg52972

  Configuring **ip flow-export template options sampler** on an ASR 1000 Router may stop Netflow from working and this may cause errors. It is not supported, so the command should be rejected at the CLI.

  This symptom is observed when configuring the unsupported feature **ip flow-export template options sampler** on an ASR 1000 Router.

  Workaround: Is to reload.

- CSCtg57720

  Junk characters are seen in the **remote address** part of "**show vpdn tunnel summary o/p"** when sessions are coming up in a new tunnel. Usually seen with 4 or more tunnels.

  Workaround: None

- CSCtg62555

  An ASR 1000 Router may be out of service after removing ip address from ip portbundle source loopback interface.

  This symptom is observed on a Cisco ASR1000 series router when functions as an Inteligent Service Gateway (ISG), when Port Bundle Host Key (PBHK) is enabled on sessions, when thousands of sessions were establishedand running high rate traffic on both upstream and downstream direction.

Workaround: There is no workaround.

- CSCtg71904

  Fragmented UDP packets with ip length =< 25 bytes are not getting encrypted.

  This condition is observed ASR 1000 forwards fragmented UDP packets with ip length =< 25 bytes out in clear text.

  Workaround: None

- CSCtg93623

  On ASR1000 Router, SBC man/sdr does not do policing properly with these steps:

  When performing the following:

  1. SBC is deactivated using **no activate**
  2. SBC configuration is removed using **no sbc global dbe**
  3. SBC is reconfigured without **control-dscp af11 marker-dscp af12 pdr-coefficient 300**

  Workaround: Is to enter these commands between steps 1) and 2) above:

  no control-dscp af11 marker-dscp af12 pdr-coefficient 300

- CSCtg94290

  Execution time of **"copy run start"** delays to 6-10 minuntes, with show tech-support simultaneously in different vty.

  Workaround: None

- CSCth04143

  When running Traditional Netflow (configured with ip flow ingress/egress), with tcp packets in the Netflow cache, if the "show ip cache ver flow" is issued, the tcp flags information will show up at the bottom of each cache entry next to the FFlags token, but the numeric value of tcp flags will be printed (incorrectly) as 0, in the tabular representation of the cache entry.

  This defect is observed when running traditional Netflow, when Netflow cache is populated with TCP packets and when the verbose form of the show command is issued i.e.

  show ip cache ver flow

  Workaround: The workaround is to read the data from the bottom of each cache entry next to the FFlags token.

  Note that the integrity of the data exported to the Netflow collector is not affected.

- CSCth08505

  Sometimes PPPoE sessions do not sync up with the Standby RP.

  This condition my occur on the first attempt when the PPPoE sessions are established and they fail to sync up with the Standby RP.

  Workaround: Reloading Standby RP may resolve this problem.

- CSCth09196

  On an ASR 1000 Router core file is generated.

  This condition is observed when accessing beyond packet data memory.

  Workaround: None

- CSCth10088

  On ASR 1000, when an invalid request of AuditValue/Modify missing termination ID is received, Context ID is missing in the ER from DBE as the reply.

  Workaround: None

- CSCth11039

  The following cli did not count the SBC flow pair statistics correctly:

  show sbc global dbe flow-pair statistics

  It used to count rejected pinholes if a command is rejected with ERR=421.

  Workaround : None

- CSCth15353

  There are few incorrect result codes seen in the VPDN system logging.

  Workaround: None

- CSCth15629

  When an ASR 1000 Router receives a IPv6 Neighbor solicitation, the resulting Neighbor Advertisement may not be seen leaving the router.

  Workaround: None

- CSCth30815

  The Result Code description for STOPCCN were incorrect.

  Workaround: None

- CSCth39877

  When L2TP tunnel on a ASR 1000 Router goes down, no syslog message was being logged for L2TP tunnel going down.

  Workaround: None

- CSCth47836

  An Cisco ASR 1000 Router may crash while processing a RTSP packet when a particular type of packet is received.

  This problem might appear while processing a RTSP packet when a particular type of packet is received, it may lead to a crash on the router.

  Workaround: None

Open Caveats—Cisco IOS XE Release 2.6.1

This section documents possible unexpected behavior by Cisco IOS XE Release 2.6.1

- CSCta46670

  When disabling and enabling **control plane host** a few times this may generate an error message on the Cisco ASR 1000 Router. This has been observed, when configuring **control plane host** followed by **no control plane host** a few times on the router.

  Workaround: None is required since there appears to be no functional impact.

- 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: None

- CSCtb98877

  On the ASR 1000 Router Series subsequent call fails after a SIP Session Refresh timeout occurs after an HA switchover in CUBE environment.

  This occurs in a back to back CUBE environment:

  CUCM1 - SIP - CUBE1 - SIP - CUBE2 - SIP - CUCM2

  The CUCM SIP Refresh is set to 90 seconds, and a call is made. HA switchover occurs on CUBE1, and the call is disconnected as expected. The same call is made again, but the originating endpoint on CUCM1 gets a Busy tone, while the terminating endpoint on CUCM2 gets Ringing tone.

  CUBE2 sends a 503 Internal error with the following cause code:

  Reason: Q.850;cause=38 - [Network out of order]

  Workaround: None

- CSCtc54288

  When changing the group number associated with a virtual IP address causes hosts to lose contact with the virtual router.

  This instance occurs when a virtual IP address is associated with one group, and then that group is unconfigured and the same virtual address used by another group. Since each group is uniquely associated with a virtual MAC address the ARP tables of all hosts that were using the previous group will contain invalid entries. When the interface is shut, while configuring new groups then gratuitous ARPs will be sent to refresh any hosts' ARP tables before the interface is ready to forward traffic. The hosts will not realize that the vIP/vMAC association in their ARP tables are invalid and will be unable to forward traffic via the known (virtual IP) gateway.

  Workaround: A delay can be used to stall the VRRP initialization process after unshutting an interface:

  vrrp delay minimum

  reload

  The values used are the number of seconds to delay, which is platform dependent. 30 seconds for interface delay and 300 seconds for reload delay are a good first values to test.

- CSCtc55215

  On the ASR 1000 Router, when shape rate is configured as % of an ATM PVC for GRE QoS it is not updated after the PVC rate has changed.

  This may occur when changes to the PVC rate and its ATM class has been configured on the router at the same time.

  Workaround: None

- CSCtc62440

  On a Cisco ASR 1000 Router Series, the removal of sub-interfaces 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.

- CSCtc69297

  Tracebacks has been seen with cli **sh platform hardware qfp active feature acl tree** on the Cisco ASR 1000 Router.

This condition has been seen, when there are a huge number of acls configured on the router.

Workaround: None

- CSCtc78745

  When deleting a few tunnels from PE side, when CE and PE are having different number of tunnels the Cisco ASR 1000 Router starts throwing msgs.

  The following message has been seen:

  ```
  Oct 27 14:33:40.170 IST: %ACE-3-TRANSERR: ASR1000-ESP(14): IKEA trans 0x1D8C; opcode
  0x60; param 0x1FD2; error 0xA; retry cnt 0
  ```

  This condition has been observed, when tunnel mismatch between CE and PE are kept for a long time on the router.

  Workaround: The are no known workaround as of now.

- CSCtc96467

  STANDBY RP reloads twice with **issu runversion**, while downgrading from Release 2.6 to 2.5.

  This instance may occur, when Super Package has been configured with ISSU, which causes the STANDBY RP to reload with **issu runversion**.

  Workaround: None

- CSCtd48042

  When defining vrfa adjacency the vrfb as singal-address is used, this can start an attack and the EP will show in vrfa blacklist on the Cisco ASR 1000 Router.

  This instance may occur, when vrfa adjacency has been defined, but vrfb as singal-address is used on the router.

  Workaround: None

- CSCtd84323

  Under Unified SBC SIP IPv6 to IPv4 scenario with DTMF digits via INFO method, the following Traceback has been seen on the console following RP failover scenario:

  ```
  "*Dec 14 20:59:14.494: %ASR1000_INFRA-5-IOS_INTR_HISTORY: [5|0] [0:0] [0->0] ra[ 1*
  0x0 1* 0x0 ] -Process= "SBC main process", ipl= 0, pid= 314".   The traceback causes a
  temporary outage in service, but SBC does recover without any manual intervention.
  ```

  This traceback has been observed in the following conditions:

  1. SIP IPv6 to IPv4 calls
  2. DTMF digits transferred via INFO method
  3. RP failover has been executed at some point in past.

  Workaround: None

- CSCtd87114

  When rate-limit is configured after msg-body, it is not shown in show logging on the ASR 1000 Router Series.

  Workaround: Is to configure rate-limit before msg-body for logging discriminator.

- CSCtd89923

  Webex SPA hard disk sectors are corrupted.

This condition has been observed when SIP10 is configured with a Webex SPA running release 2.6.0 image that is Soft-OIR'ed. This configuration can potientially corrupt the sectors on the hard disk of the Webex SPA.

Workaround: Is to shutdown the SPA before reloading the SIP10.

- CSCtd91015

  The Cisco ASR 1000 Router does not roll back to the base image even though the rollback timer has expired for ISSU Superpackage Downgrade from Release 2.6 to 2.5. ISSU Superpackage Downgrade does not finish within the specified “roll back” time, but router does not rollback to the base image. Tracelogs shows that the timer has been expired and a user prompt has appeared. But the prompt does not appear on the console. SPA's will move to “inserted” mode and at certain times STANDBY RP will reload.

  Workaround: ISSU will work fine, when rollback time is increased.

- CSCtd92548

  On the Cisco ASR 1000 Router Series when issuing “issu runversion” the FP, ccp_cp_svr cores on the new Active RP.

  This conditions may occur while doing super package issu, after issuing "issu runversion", cpp_cp_svr cores on the new active RP. This has been seen on the multidimensional scaled environment where as both PPPoEQinQ and PPPoEoA are configured on the same Cisco ASR 1000 Router.

  Workaround: None

- CSCte01388

  The FMAN FP process may crash on the ASR 1000 Router Series.

  This has been observed, when VPN has been configured on the router.

  Workaround: None

- CSCte07777

  The ASR 1000 Router Series may face HQF clean up issues within a QoS ATN PVP enviroment.

  This condition may happen on a Cisco ASR 1000 Router when runnning pre-released image.

  Workaround: None

- 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.

- CSCte28845

  With Cisco ASR 1000 Router operating in uSBC mode, all adjacencies are locked in Detached state after an upgrade or change where the SBC must be deactivated and activated.

  When SBC is deactivate or activated or the same for one of the adjacencies, the system prints a routing error log.

  The problem occurs when there is an digit routing entry in the routing table that is missing the destination adjacency datafill.

In most cases the SBC will not allow this to be configured in the first place without throwing an error but there are some scenarios where this configuration can get into the database without an error.

Workaround: Remove the entry with “no dest adjacency” or “add a dest adjacency” to the entry datafill.

- CSCte48047

  On a ASR 1000 Router Series the output from the **sh platform software status control- processor** may incorrectly indicate that the ESP committed memory is greater than 100%. There is no functional impact due to this.

  Workaround: There are no known workarounds.

- CSCte49434

  Upon doing RP switchover on the Cisco ASR 1000 Router, the following error messages are seen on the RP console:

  *Jan 18 19:11:13.860: %IOSXE-3-PLATFORM: R1/0: kernel: /scratch/mcpre/BLD-BLD_V122_33_XNF_ASR_RLS6_THROTTLE_LATEST_20100118_180012/os/linux/drivers/binos/i2c/pca9535/pca9535_main.c:set_reg_output_port_0 (line 185): write pca9535 register at 02 failed

  *Jan 18 19:11:13.882: %CMRP-3-I2C_WRITE: R1/0: cmand: An I2C write has failed because Input/output error -Traceback= 1#4800cc02ea45b52bc53dc957092af093 errmsg:EDA4000+2160 :10000000+24608 :10000000+4C354 :10000000+4A1AC :10000000+46FEC :10000000+47598 :10000000+492F0 :10000000+49B2C evlib:F15B000+D854 evlib:F15B000+FF74 :10000000+311E4 c:E53C000+1D078 c:E53C000+1D220

  Conditions: This problem has been seen on the a Cisco ASR 1006 Router with redundant RP's when the command **“redundancy force-switchover”** is issued. This problem has been seen very infrequently.

  Workaround: There is no workaround. This problem is not affecting the function of the router.

- 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: None

- 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: None

- 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: None

- CSCtf04444

  L2TPv3 sessions do not come up on a Cisco ASR 1000 Router.

  The condition sessions do not come up when copying l2TPv3 xconnect on the same Gige interface that used an MPLS xconnect. earlier.

  Workaround: Is to write the new l2tpv3 config on nvram and reload the router.

- CSCtf05408

  IP address on a loopback interface is lost on the Cisco ASR 1000 Router Series.

  Workaround: Is to reconfigure the loopback interface.

- CSCtf07876

  The following error message may appear on the ASR 1000 Router console:

  %IDBINDEX_SYNC-4-RESERVE: Failed to lookup existing ifindex for an interface on the Standby, when allocating a new ifindex from the Active.

  This error message has been observed after SSO.

  This problem may occur after deleteing some configured TE tunnels and when using SSO.

  Workaround: None

- CSCtf13608

  ESP Kernel crashes when using Release 2.6 image on the ASR 1000 Router Series.

  Workaround: None

- CSCtf13925

  CPP back pressures n2 occurs on the FP10.

  This can impact performance when using IPSEC/SSL on the FP10.

  This condition occurs on every record n2 returns to CPP.

  Workaround: None

- CSCtf16427

  Pending objects seen while churning ANCP sessions on a Cisco ASR 1000 Router.

  This condition are seen when the ASR 1000 Router has been configured with Model F with PPPoEoA ANCP sessions.

  In addition, pending objects are seen after churning the ANCP sessions.Workaround: There is no known workaround.

- CSCtf19360

  Memory Leak are seen when processing Crypto IKMP.

  This condition can occur when Vrf Aware EZVPN has been configured on the ASR 1000 EzVPN-Server

  Workaround: None

- CSCtf27659

  After 3 to 4 RP switchovers with a 480 sec sleep in between each RP switchover, the flow-control ids on the active and standby RP are out of synch with the following error:

  ```
  Feb 23 17:29:27.418: %ASR1000_RP_SPA-3-VC_FLOWID_ALLOC_FAIL: Failed
  to allocate a flow control identifier for VC 16871576under interface ATM0/1/0
  ```

  As a result of which all 32k PPPoEoA sessions do not get established.

  This condition has been seen when RP switchover causes the flow-control ids on the active and standby RP to be out of sync, and thus not all sessions getting established.

  Workaround: Is to reload the router.

- CSCtf36152

  When ASR(LAC) receives StopCCN from LNS due to the lack of resources (L2TP session limit), the ASR (LAC) returns ZLB with bad sequence number.

  In this case, the correct Ns/Nr of ZLB should be Ns=1/Nr=1.

  Workaround: None

- CSCtf51834

  After a stateful switchover (SSO) on an IOS router supporting L2TP HA, the counter showing the number of L2TP sessions which were destroyed because they were not completely established at the time of the SSO, may be incorrect.

  This counter is visible with the command show l2tp redundancy detail in the section Sessions destroyed during resync phase.

  For example, the sessions destroyed during resync phase:

  ```
  Poisoned:         0
  Unestablished:    10    -- This value may be incorrect
  Tunnel in resync: 0
  ```

  After a stateful switchover (SSO) on an IOS router supporting L2TP HA.

Workaround: No workaround.

- CSCtf65681

  This is for CUBE(SP Edition), an SBC application on the ASR 1000 Router Series.

  The SBC service failed after receiving a SIP REGISTER response.

  This happens when the response comes with a strange expire value, 0xFFFFFFFF.

  Workaround: There is no work around on CUBE(SP Edition). But the customer should isolate the entity sending 0xFFFFFFFF as the expire value and disable it.

  That is not a normal vale.

- CSCtf69311

  Phase2 tunnel History Table MIB values for VRF Aware IPSec is not fetched on the ASR 1000 Router.

  This condition may happen when VRF Aware IPSec configuration on UUT and Phase2 IPSec tunnel is cleared with <clear crypto session>.

  Workaround: None

- CSCtf69391

  Output drops on an interface incrementing apparently due to ISG with session drops.

  Conditions: Low traffic may be seen on the interface. This is alarming in that these appear to be actual packet drops from traffic.

  Workaround: None

- CSCtf70393

  This is a minor problem with CUBE(SP Edition), a SBC service running on the ASR 1000 Router Series.

  The is no reason counter increased when SBC rejecting SIP incoming call with 503 response.

  This problem happens when certain internal resource is running out because of ongoing signaling traffic.

  Workaround: This does not bring down the SBC service, just missing counter.

- CSCtf70450

  Very low performance when reassembling MPLS traffic.

  This condition has been seen when enabling ‘mpls mtu max’, then runnning EoMPLSoGRE traffic.

  Workaround: None

- CSCtf74687

  MEGACO errors 421 and 430 observed on the RP.

  This condition are seen in a RP switchover scenario, under high load.

  Workaround: None

  Further Problem Description: When calls are not fully setup at the time of switchover will not have been replicated to the standby, resulting in 430 when the MGC sends subsequent messages after the switchover. There is also a timing window where replication information is 'in-flight', and gets lost at the time of switchover, resulting in 421 when the MGC attempts to MODIFY the gate after switchover. Both of these symptoms are normal and expected in the course of operation. The increased TAT is a function of the increased load in this environment.

- CSCtf75746

The ASR 1000 RP2 core when using "**no sbc**" and this can happen sometimes, not everytime.

This appears to happen because a call is waiting for a buffer to send a message, and then the SBC is deactivated. When the buffer comes in, this assert is seen because the call is no longer exists.

Workaround: None

- CSCtf77225

  PBR counters under **sh route-map dynamic** shows inconsistency, sometimes the counters increment and sometimes it shows "0".

  The traffic class being monitored is "INPOLICY", and traffic is being forwarded appropriately.

```
6RU_BR2#sh route-map dynamic
route-map OER_INTERNAL_RMAP, permit, sequence 0, identifier 922746881
Match clauses:
ip address (access-lists): oer#1
Set clauses:
ip next-hop 200.1.1.2
interface GigabitEthernet0/1/5
Policy routing matches: 0 packets, 0 bytes --->>>> no matches
Current active dynamic routemaps = 1
6RU_BR2#sh mpls forwarding-table | i 90.1.1
22         No Label   90.1.1.0/24      84075         Gi0/1/0    14.1.1.2    ---->>
packets being forwarded
6RU_BR2#
```

  Workaround: None

- CSCtf84496

  ESP might generate fman-fp-image core when remote peers have burst with aggressive IPSec rekey activity.

  This condition has been observed when 2K svti crypto session flaps per 30 seconds.

  Workaround: None

- CSCtf93465

  In a CUBE(SP Edition) ASR 1000 Router, the following message is seen when trying to enter SBC config mode:

```
SBC: Internal error - SBC configuration cannot be processed.
```

  This condition sometimes happens after unconfiguring SBC.

  Workaround: The workaround is to do a reload.

- CSCtf95136

  SIP notify to RFC2833 DTMF interworking failed.

  SBC did not correctly signal DTMF interworking capabilities in a flow where SBC is configured to support DTMF NOTIFY for the caller.

  This condition has been seen when n 2000K sends from SBC to caller side, there is no call-info header.

  Workaround: None

- CSCtg04257

  After SBC hit the system congestion the following messages are seen on the console:

```
*Apr  3 02:06:34.956: %SBC-2-MSG-3802-0432-BA2C8E-1302: SBC/SIP:
SBC is currently congested and is rejecting new call requests.
*Apr  3 02:06:37.966: %SBC-2-MSG-3802-0432-BA2C8E-1302: SBC/SIP:
```

```
SBC is currently congested and is rejecting new call requests.
```

Then SBC quits to process all the messages. This problen may occur when congestion occurs on a Cisco ASR 1000 Router .

Workaround: None

- CSCtg07737

  More than 70 sec multicast traffic loss occurred after performed CC software OIR.

  Workaround: None

- CSCtg09182

  FMAN traceback messages are seen on the Cisco ASR 1000 Router console:

  ```
  %FMFP_URPF-3-LIST_DOWNLOAD: F1: fman_fp_image: Unicast RPF list create for list 10594
  fail to download because No such file or directory.
  ```

  This condition may occur when the ASR 1000 Router has 6000 subscribers Loaded with stateful traffic from an IXIA, 15000 vanilla PPP (pass policy) in V-T 4, 2500 flapping subscribers with FW, and 2500 flapping subscribers with no firewall. The failure is on a 10G interface carrying MPLS.

  Workaround: There is no known workaround.

- CSCtg16498

  LNS VPDN message is incorrect when receiving CDN from LAC as follows:

  ```
  %VPDN-4-SESSIONERROR: L2TP LNS R102 unable to terminate user cisco@cisco.com; Result
  1, Error 0, No disconnect reason given
  ```

  It should start with "%VPDN-4-SESSIONERROR: L2TP LAC".

  This occurs when receiving CDN's result code is "1" and the following is configured on the router:

  vpdn logging is enabled

  Workaround: There is no workaround.

- CSCtg21602

  In this example the following message is displayed on the Active RP Console:

  ```
  %CPPOSLIB-3-ERROR_NOTIFY: F1: cpp_cp:  cpp_cp encountered an error -Traceback=
  1#ed4b69bc77a25ff35c522388cbb72a96   errmsg:D94E000+2160 cpp_common_os:E0A4000+B920
  cpp_common_os:E0A4000+19148 cpp_exmem_mgr:ED1E000+895C cpp_exmem_mgr:ED1E000+9080
  cpp_common_os:E0A4000+163D0 cpp_rrm_local_api_lib:EFDF000+3150
  cpp_rrm_svr_lib:F004000+53F0 cpp_rrm_svr_lib:F004000+76CC cpp_rrm_svr_lib:F004000+80A4
  cpp_rrm_svr_lib:F004000+9810 cpp_dmap:E954000+15264 cpp_dmap:E954000+21BF4
  cpp_common_os:E0A4000+
  ```

  This message is displayed right after un-configuring sbc by entering command:

  no sbc global dbe

  Workaround: None

- CSCtg30995

  Delay of RP switchover associated with NV_BLOCK_INITFAIL message appearing on standby-turned-active RP console.

  When the manual switchover command, **redundancy force-switchover** and a filesystem command like **copy running-config startup-config** is issued from different consoles of active RP almost at the same time, such a problem may occur.

Workaround: Avoid issuing any filesystem access command simultaneously with the manual RP switchover command. Should the above problem occur, please execute the same filesystem command, say, **copy running-config startup-config** from the standby-turned-active console.

- CSCtg37082

  Following warning messages are seen on active RP upgrade (ISSU) and switchover after upgrading to Release IOS XE 2.6.1 from 2.3.0e:

  %IMRP-3-IMRP_MSG_CANNOT_RELAY: R1/0: imand: IMRP Peer ios_rp_iosd_slot_1:

  cannot relay message to SPA 15/15

  %IOSD_IMCC_CAPI-3-MSGDISPATCH: SIP2/1: Unable to dispatch received TDL

  After ISSU upgrading the active RP to IOS XE Release 2.6.1 from 2.3.0e, when RP switchover is initiated this warning will be seen on the newly active RP.

  The warning messages do not affect the general working of the SPA during ISSU when the VLAN Tunnel mode feature is not used.

  Workaround: None

- 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

Resolved Caveats—Cisco IOS XE Release 2.6.1

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.6.1

- CSCso88429

  CME or CUBE will reject an inbound SIP INVITE if Max-Forwards is greater than 70.

  The symptoms are observed when a Max-Forwards header field in SIP INVITE is greater than 70.

  Workaround: There is no workaround.

  Further Problem Description: From RFC 3261: 20.22 Max-Forwards

- CSCsq24672

  A call through CUBE may not establish for a Re-Invite-based call flow. The call may drop.

This symptom is observed if the endpoint to which the CUBE is communicating sends a Re-INVITE for a call before it has received an ACK from the other call leg for the original INVITE. CUBE may not forward this Re-Invite to the other call leg, and the call will disconnect.

Workaround: There is no workaround.

- CSCsq57238

  An interface is congested. A QoS policy-map is applied to the interface such that one of the traffic-classes receives only infrequent packets. That traffic class is seen to have higher than expected latency. If steady traffic is sent through the same traffic class, then latency is as expected and bandwidth is seen to be shared between traffic classes as per their relative bandwidth guarantees.

  The symptoms are observed on any interface, but is most obvious with low speed interfaces such as ATM PVCs with 256k or less bandwidth.

  Workaround: If the traffic class with the infrequent traffic in configured with **"priority"**, then latency will be minimized.

- CSCsv98245

  The output of the "show ip bgp neighbor x.x.x.x advertised-routes" displays "Originating default network 0.0.0.0" even when default network is not expected to be originated.

  This may be seen in the **"show ip bgp neighbor x.x.x.x advertised-routes"** output, even if there are no routes being advertised, as shown in the example:

```
Router# show ip bgp neighbor 10.0.10.10 advertised-routes
BGP table version is 3, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
Originating default network 0.0.0.0
Network          Next Hop            Metric LocPrf Weight Path
Total number of prefixes 0
```

  Workaround: No workaround.

- CSCsx66105

  Chunk memory leaks at "SADB SA Header" are seen on the Group Member. The memory leaks are seen when ipsec SAs are cleared using the command "clear crypto gdoi"

  Workaround: No Workaround

- CSCsz07615

  When **reload** cli is issued it takes some time to gracefully bring down the system. In this process it will unusually take longer time for redundancy protocols to notify its peers and cause few timing issues.

  This has been onlyobserved when redundancy protocols like HSRP are seen to misbehave.

  Workaround: Is to bring down the system instead of gracefully reloading.

- CSCsz69148

  When running an embedded syslog manager (ESM) TCL script on the ASR to filter logs, memory leaks in IOSD ipc task and ESM Logger occur. This memory leak applies to RP1 and RP2. Any feature which uses heavy logging (for example, audit logging for firewall features) will exploit this issue readily.

  Workaround: There is not current workaround other than to no use the ESM feature.

- CSCsz82950

On the Cisco ASR 1000 Router a peer RP reloads. If any configurations are done using NMS for DCTM MIB, this symptom occurs when unconfiguring the configuration that is created by DCTM MIB configuration.

There is no workaround.

Further Problem Description: DCTM was not HA supported before. HA is supported

- CSCta21525

  High CPU is seen when sending SNMP queries to a router just configured to send TRAPS. The host sending the query must have the correct TRAP community.

  When configuring: **'snmp-server host 10.13.37.1'** , the router will start to listen to SNMP-requests sent to the router. The router sets the community to public if nothing else is specified.

  Workaround: Is to secure SNMP with the use of ACL's & and add a more seucre SNMP community for the above command.

- CSCta26492

  OSPFv3 does not advertise prefixes ralated to virtual-access interface on a Cisco ASR 1000 Router.

  This hase been seen when configuring **"ipv6 ospf"** under virtual-template on the router.

  Workaround: configuring "redistribute connected"

- CSCta58068

  During BGP convergence, CPU spike may be seen on the local PE in an MVPN configuration after conditions.

  This condition happens to cause excessive BGP convergence and high CPU utilization (with and without traffic) in an MVPN setup can be varied as:

  -Remote PE neighbor switchover

  -On local PE, while doing a "clear ip bgp <bgp nbr>".

  -On bringing up the local PE

  -Large configuration such as one with 300 MDT default tunnels.

  Here is an example of an MVPN configuration where this problem can be exhibited:

  1. OSPF routing protocol is enabled on all the networks in the topology.
  2. Each PE router, has 100 MVRFs defined (between vpn_0 to vpn_99).
  3. MDT default is configured on all the mVRFs on the PE routers.
  4. PE routers have an iBGP session, ONLY with the RR (route-reflector).
  5. eBGP session exists between the Routem and PE1, with Routem sending 200,010 VPNv4 routes.
  6. OSPF session also exists between Routem and PE1, with Router sending 100 OSPF routes.

  In effect the following states are present in the network:

  On PE and RR routers:

  1. IGP states = 100 OSPF routes
  2. BGP states = 200,010 VPNv4 route

  On PE routers ONLY:

  1. VRF sessions = 100 VRFs (vpn0 to vpn_99
  2. MDT sessions = 100 SSM session

Workaround: None.

- CSCtb05810

  When applying the no distance command, the summary-prefix disappears from the route table. When you check the OSPFv3 database, the summary route exists.

  Workaround: Is to configure summary-prefix command again.

- CSCtb62351

  The output of '**show ip vrf detail <*vrf_name*>**' shows the number of routes greater than the actual number of routes in a VRF.

  This problem happens when the route count does not get updated correctly when a route with a better distance replaces an existing route only occurs when the route in question is also a major network.

  Workaround: Is to issue the command '**clear ip bgp vpnv4 vrf *'.**

- CSCtb62689

  When system is congested and a switchover occurs SBC drops calls instead of answer with the SIP congestion message 503 that indicates that the system is congested.

  The problem only occurs after a switchover of a congested system.

  Workaround: None

- CSCtb86371

  TCP packets from client requiring PBHK are silently drop by ISG router.

  After a TCP connection is idle with no activity for more than 60 seconds, the PBHK portmapping will be removed to protect the ISG from losing memory on lost connection. However if a client tries to use an existing TCP conneciton it has with a server after a 60 seconds of inactivity, those packets are dropped, giving a hang TCP connection. The behavior expected by ISG should be to return a TCP RST.

  Workaround: Is to force a reset or close the TCP client connection.

- CSCtb89424

  In rare instances, a Cisco ASR 1000 Router may crash while using IP SLA udp probes configured using SNMP and display an error message similar to the following:

  hh:mm:ss Date: Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x424ECCE4

  This symptom is observed while using IP SLA on the router.

  Workaround: There is no workaround.

- CSCtb94498

  The RP resets at IGMP Input on a Cisco ASR 1000 Router.

  This issue has been seen only when repeated config and unconfig of the VRFs is performed.

  Workaround: The issue will not be seen if there is more than 5secs time delay between the config/unconfig.

- CSCtb96865

  When LAC fails to attempt to establish L2TP session, it will add LNS's ip addresses to dead cache entry, even if the reason of failure due to LAC internal error. The LNS's ip-address will be put on busy list for 60 seconds due to this.

  This conditon has been seen when LAC has internal failure and fails to create l2tp tunnel to lns.

Workaround: There is no known workaround.

- CSCtc12904

  A crash in IPv6 ND processing a timer wheel on the Cisco ASR 1000 Router.

  This is a very rare condition that might happen as a neighbor is removed from the ND cache.

  Workaround: None

- CSCtc18656

  When the NAT box is configured as the Rendezvous Point (RP). This does not allow for source address translation for the encap packet received from the First Hop Router. NAT box is configured as Rendezvous Point (RP) decapsulates the packet and forwards it to NAT outside without translation which will create incorrect S,G state for a inside local source address on the downstream routers after NAT router.

  Workaround: None

- CSCtc31545

  Some EIGRP routes may not be installed in the routing table after a link flaps. The route is seen as “active” in the EIGRP topology table, and the active timer is “never”.

  This has been seen when a backup path has an EIGRP composite metric of infinity and the primary path is flapping.

  Workaround: Is to use realistic metrics for all paths rather than very high delay values which may result in an infinite metric. Once in this condition, the only way to resolve the issue is to clear the neighbors.

- CSCtc35416

  VPDN debugs are enabled on the ASR 1000 Router Series. When username conditional debugging is **enabled**, VPDN debugs should not be printed, but a few debug messages are still seen.

  Workaround: None

- CSCtc37349

  Under router distribute-list prefix command ACL option is shown. Which is not correct.

  As a result the access list is configured, which has prevented configuring prefix name with numbers.

  This condition are seen when router ospf 10 distribute-list prefix in used on the ASR 1000 Router.

  Workaround: None.

- CSCtc42941

  On a Cisco ASR 1000 Router the Standby is not coming up.

  When a distribute-list is configured, the ACL is created if it does not exist. Then remove the ACL, but the distribute-list configuration that ties to the ACL is not removed. Configure the IPv6 ACL configuration with the same ACL name. Save the configuration and reload it.

  Workarounds:

  1. When a access list is removed, remove corresponding distribute-list configuration as well.
  2. Do not use the same access list name for IPv4 and IPv6.

  Further Problem Description: Is to use router bgp 100 distribute-list sample in exit and no ip access-list standard sample ipv6 access-list sample permit any write to the memory.

- CSCtc51539

  A Cisco ASR 1000 Router crashes with a “Watch Dog Timeout NMI” error message.

This symptom is observed only on devices configured with Bidirectional Forwarding Detection (BFD). For further information on BFD, consult the following link: http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

Workaround: Is to disable BFD.

- CSCtc57356

  IOS SLB natpool will source nat addresses outside the range specified in config.

  This has been observed when IOS SLB with client nat and a nat pool with same address as start and end range and 31 bit mask.

  Workaround: s to USE 2 (two) ip addresses in range and not not allow for other devices including backup IOS SLB or other slb in same network to use the same range.

- CSCtc68037

  A Cisco ASR 1000 Router device may experience an unexpected reload as a result of mtrace packet processing.

  Workaround: None other than avoiding the use of mtrace functionality.

- CSCtc87430

  The following errors are seen on Active RP during RP switchover with scaled sessions(around 5k):

  “asr1000 bsess: RPC header processing failed, error=5001”

  This conditions are seen in an environment that is using the following setup:

  Agilent--->(atm)--->ASR 1000 Router ---->(10GB)----->LNS(c10k)----->Agilent

  and with the following configurations as shown in this example:

  1. Configure the Cisco ASR 1000 Router as LAC with Model D2.1 QOS
  2. Start session bring-up
  3. At aroung 5k session, issue RP SWO
  4. Noticed errors on new Active RP

  Workaround: None

- CSCtd24065

  The output of the command **show subscriber statistics** shows that number of “SHDBs in use” is greater than the total number of unique subscribers for the deployment. This might contribute to issues such as an “out of IDs” message or sessions not coming up.

  The symptom occurs for DHCP-initiated sessions either when:

  1. Session idle times out followed by a lease expiry or you release the lease.
  2. Session is cleared using the **clear subscriber session** command and there is a lease expiry or you release the lease.

  Workaround: There is no workaround.

  Further Problem Description: This can also contribute to a small amount of observed memory leak. This problem occurs in code branches where IP session HA is not supported. In these branches, the above steps cause a SHDB handle to not be cleared properly when other datastructures are cleared.

- CSCtd25664

  ERSPAN session are not sending traffic to the analyser on the Cisco ASR 1000 Router Series. ERSPAN session are not filtering traffic as expected on the router.

This condition has been observed, when the Cisco ASR 1000 Router is running 12.2(33)XND1 and previous versions.

1. ERSPAN configured with vlan filtering
2. ERSPAN configured with vlan sourcing

Workaround: Is to do the following:

1. Filter traffic on the analyser
2. There is no known 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 <i*f_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.

- CSCtd33780

  When there are two vrfs A (exporting) and B (importing), admin shutting down the neighbor under vrf A while doing:

  'sh ip bgp vpnv4 vrf seven <*prefix_learned_from_neighbor_shut_under_vf_one*>' with auto-more causes the Cisco ASR 1000 Router to crash.

  This condition are seen for this timing issue, the following events MUST happen VERY FAST to be reproduced:

  1. Add vrf "seven" which imports paths from existing vrf (vrf "one")
  2. Admin **shut** the neighbor under vrf "one" while simultaneously doing

  '<sh ip bgp vpnv4 vrf seven <*prefix_learned_from_neighbor_shut_under_vf_one*>'

  with auto-more in another terminal

  Workaround: No workaround.

- CSCtd36639

  The following traceback are seen %ASR1000_INFRA-5-IOS_INTR_OVER_LIMIT while running overnite with 64 groups and 1500 OIF's each with no traffic:

  %ASR1000_INFRA-5-IOS_INTR_OVER_LIMIT: IOS thread disabled interrupt for 17 msec

  -Traceback= 1#cbbad1ee0e5052dcf6fb7a00f91e7a88 :400000+D1A6A9 :400000+40476FD :400000+404849B :400000+250CF16 :400000+250CD07 :400000+2510305 :400000+15941A7 :400000+41067B0 :400000+41064D6

  This conditions keeps a scaled configuration running overnight without any traffic.

  Workaround: None

- CSCtd43965

The command **snmp context** <*context*> is not available to be configured for EIGRP multicast address-families. Furthermore, on images that support EIGRP multicast address-families but do not have the EIGRP MTR (Multi-Topology Routing) plug in, this command is not available to be configured for EIGRP unicast address-families either. As a result, it is not possible to associate these address-families with a specific SNMP context.

This conditions are affects of any image that has EIGRP release 2.5 or later code and supports EIGRP multicast address-families.

Workaround: No workaround.

- CSCtd48455

  When "ip summary-address eigrp ..." advertises a subset of component routes in addition to the summary.

  This symptom happens when the number of redistributed prefixes extends beyond approximately 100 routes.

  Workaround: Is to do the following:

  1. Assign an IP address which is a component of the summary to a connected interface; ie. a loopback interface.
  2. Run **clear ip eigrp neighbor soft** (will not reset adjacency) **clear ip eigrp neighbor** (will reset adjacency)

  Further Problem Description: This problem reappears if **clear ip route * is executed**.

- CSCtd48480

  Memory leak are seen in the function ppp_aaa_apply_peruser_attributes.

  This condition are seen while initiating and clearing ppoe call consecutively resulting the memory leak.

  Workaround: No workaround.

- CSCtd54970

  Internal routes may only be tagged with values less than or equal to 255. With this defect, the tag was allowed to be set to higher values if a route-map was applied outbound on a specified interface.

  Whe the outbound route-map is applied to a specific interface with set tag great than 255 for internal routes.

  Workaround: Set tag to a value less than or equal to 255.

- CSCtd56668

  The Cisco ASR 1000 Router retains Multicast MAC entry in HSRPDA TCAM even after port 'shut'. This may possibly lead to packet duplication.

  When virtual MAC is added to HSRPDA TCAM of active RP upon configuring HSRP between two ASR 1000 Routers. This entry persists after port **shut** on the active.

  Workaround: There is no known workaround.

- CSCtd61194

  When configuring ERSPAN on FastEthernet, gives an error:

  "SPAN is not supported on SPA interface"

ASR1K(config-mon-erspan-src)#source interface ?FastEthernet FastEthernet IEEE 802.3GigabitEthernet GigabitEthernet IEEE 802.3z Port-channel Ethernet Channel of interfaces TenGigabitEthernet Ten Gigabit Ethernet ASR1K(config-mon-erspan-src)#source interface fastEthernet 0/3/0 SPAN is not supported on SPA interface (FastEthernet0/3/0)ASR1K(config-mon-erspan-src)#

Conditions: This condition has been observed when running release Version 2.4.1.

Workaround: Is to Use GigabitEthernet.

- CSCtd63242

  A traceback or crash may be seen when deleting a subinterface that has IPv6 EIGRP running on it.

  This condition are seen when ipv6 eigrp ***<as>*** is configured on a subinterface and the a **no interface** ***<subinterface>*** is entered.

  Workaround: Is to Remove eigrp from the subinterface with a ""no ipv6 eigrp <AS>"" before deleting the subinterface.

- CSCtd66013

  On Cisco ASR 1000 Service Series Routers, Last reload reason: 4 is displayed in show version output after power-cycle.

  This symptom is observed after RP switchover and then power-cycle.

  Workaround: None. This issue is cosmetic and does not affect traffic and operation on the router.

- CSCtd66189

  Route-map with 'set pv6 next-hop peer-address' in 6PE setup sets wrong NH, such as A00:4D:: (for ipv4 address of the peer 10.0.0.77) insead of ::FFFF:10.0.0.77 - ipv4-mapped address. Route-map with 'set pv6 next-hop peer-address' can be either incoming or outgoing

  Workaround: None known at this time

- CSCtd68197

  Memory leak might be seen in IPv6 RIB Redistribute process.

  This happens when the router has ipv6 eigrp neighbor and has some ipv6 eigrp router.Memory leak might be seen with following step.

  1. When changing ipv6 address for loopback interface on ipv6 eigrp neighbor router.
  2. Shutdown the connected interface on ipv6 eigrp neighbor router. --> reducing the holding of IPv6 RIB Redistribute.
  3. No shutdown thNe connect interface on ipv6 eigrp neighbor router. --> returning the holding value.
  4. Repeat to 1.

  This is ONLY seen when an ipv6 eigrp process is partially configured. If fully configured, it does not occur and thIs is the easiest workaround to make sure that the eigrp process is configured and there are interfaces participating (even just a loopback) with that eigrp process (**sh ipv6 eigrp** <*asnum*> **interface**). Reproducibility is not 100%, but after 2. or 3. operation, sometimesholding value might be increased from previous value of same condition.

  Workaround: Is to - configure the IPv6 eigrp process completely - deconfig IPv6 eigrp process that is not running.

- CSCtd69644

  ISSU scripts indicate load version failure due to WMA SPA being offline.

While, attempting a superpkg issue upgrade, when we issue an ISSU load version command, the WMA spa seems to dissappear from the output of the ""show hw-module subslot all oir"" command for a few seconds, only to re-appear later after approx 15-20+ seconds. This causes the ISSU libraries to indicate that not all SPA's came online after loadversion. This issue is not seen with the GE, POS, CT3 SPA's in the system.

Workaround: Suggested workaround is to wait for 15-20 seconds after load version completes, prior to checking the output **of show hw-module subslot all oir** command to verify WMA SPA coming online.

- CSCtd70582

  Traffic Class services will remain in **show subscriber session** output under “Policy Information” after traffic class has disconnected by timer events.

  This conditions are only seen when Traffic Class is disconnected through an Idle Timer or Absolute Timer expiring.

  Workaround: If traffic class service is disconnected through normal (User Intervention), issue is not seen. For Timer disconnected Traffic Class services, no known workaround at this time.

- CSCtd72441

  On a Cisco ASR1000 series router, when the command **show platform software wccp *<service-id>* counters** is executed, the obj_id field in the output in rare situations maybe a large negative number. It is a cosmetic issue and does not affect functionality.

  This condition are seen when WCCPv2 is configured on the router and is redirecting traffic. The object id value is greater that 2147483647. The command **show platform software wccp *<service-id>* counters** is executed

  Workaround: There is no workaround. However there is no functionality impact.

- CSCtd73567

  The Cisco ASR 1000 Router Series may reload unexpectedly while reassembling a fragmented ip packet.

  Workaround: None

- CSCtd75033

  Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability.

  Note Note: The fix for this vulnerability has a behavior change affect on Cisco IOS Operations for Mode 7 packets. See the section Further Description of this release note enclosure.

  Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

  ntp master *<any following commands>*

  ntp peer *<any following commands>*

  ntp server *<any following commands>*

  ntp broadcast client

  ntp multicast client

  The following example identifies a Cisco device that is configured with NTP:

```
router#show running-config | include ntp
```

```
ntp peer 192.168.0.12
```

The following example identifies a Cisco device that is not configured with NTP:

```
router#show running-config | include ntp
router#
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the show version command to display the system banner. The system banner confirms that the

device is running Cisco IOS Software by displaying text similar to “Cisco Internetwork Operating System Software” or “Cisco IOS Software.” The image name displays in parentheses, followed by “Version” and the Cisco IOS Software

release name. Other Cisco devices do not have the show version command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
 Cisco Internetwork Operating System Software
 IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
 Technical Support: http://www.cisco.com/techsupport
 Copyright ) 1986-2008 by cisco Systems, Inc.
 Compiled Mon 17-Mar-08 14:39 by dchih
 <output truncated>
```

The following example shows a product that is running Cisco IOS Software

release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version
12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link:

http://www.cisco.com/warp/public/620/1.html

Workaround: There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Note Note: NTP peer authentication is not a workaround and is still a vulnerable configuration.

* NTP Access Group

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

```
!--- Configure trusted peers for allowed access
access-list 1 permit 171.70.173.55
!--- Apply ACE to the NTP configuration
ntp access-group peer 1
```

For additional information on NTP access control groups, consult the document titled "Performing Basic System Management" at the following link:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

*** Infrastructure Access Control Lists**

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks.

Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: Network Time Protocol (NTP)
!---
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
 INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
!--- Note: If the router is acting as a NTP broadcast client
!---   via the interface command "ntp broadcast client"
!---   then broadcast and directed broadcasts must be
!---   filtered as well.  The following example covers
!---   an infrastructure address space of 192.168.0.X
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 255.255.255.255 eq ntp
!--- Note: If the router is acting as a NTP multicast client
!---   via the interface command "ntp multicast client"
!---   then multicast IP packets to the mutlicast group must
!---   be filtered as well.  The following example covers
!---   a NTP multicast group of 239.0.0.1 (Default is
!---   224.0.1.1)
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 239.0.0.1 eq ntp
!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.
access-list 150 deny udp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations.  Permit all other traffic to transit the
!--- device.
access-list 150 permit ip any any
!--- Apply access-list to all interfaces (only one example
!--- shown)
interface fastEthernet 2/0
 ip access-group 150 in
```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control List" presents guidelines and recommended deployment techniquesfor infrastructure protection access lists and is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

*** Control Plane Policing**

Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, whilst the second looks at rate limiting NTP traffic to the box.

– Filtering untrusted sources to the device.

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses.

Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```
!--- Feature: Network Time Protocol (NTP)
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD any eq 123
!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.
access-list 150 permit udp any any eq 123
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
class-map match-all drop-udp-class
 match access-group 150
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
policy-map drop-udp-traffic
 class drop-udp-class
 drop
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
control-plane
service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function.

– Rate Limiting the traffic to the device

The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

Warning **Warning: If the rate-limits are exceeded valid NTP traffic may also bedropped.**

```
!--- Feature: Network Time Protocol (NTP)
access-list 150 permit udp any any eq 123
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
class-map match-all rate-udp-class
match access-group 150
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
!--- for more information on choosing the most
!--- appropriate traffic rates
policy-map rate-udp-traffic
class rate-udp-class
police 10000 1500 1500 conform-action transmit
exceed-action drop violate-action drop
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
control-plane
 service-policy input drop-udp-traffic
```

Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S - Control Plane Policing” at the following links:

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

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

Further Description: Cisco IOS Software releases that have the fix for this Cisco bug ID, have a

behavior change for mode 7 private mode packets.

Cisco IOS Software release with the fix for this Cisco bug ID, will not process NTP mode 7 packets, and will display a message “NTP: Receive: dropping message:

Received NTP private mode packet. 7” if debugs for NTP are enabled.

To have Cisco IOS Software process mode 7 packets, the CLI command <cmd>ntp allow mode private</cmd> should be configured. This is disabled by default.

This is the same as the vulnerability which is described in:

http://www.kb.cert.org/vuls/id/568372

Cisco has release a public facing vulnerability alert at the following link:

http://tools.cisco.com/security/center/viewAlert.x?alertId=19540

Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE and 15.0(1)M.

All other versions of Cisco IOS and Cisco IOS XE Software are affected.

To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returnseither of the following commands listed then the device is vulnerable:

- CSCtd86572

DMVPN EIGRP topology hub does not update spoke with new next hop information for prefix with equal cost paths.

This condition may happen when dual hubs are setup where each spoke only peers with one hub and hubs exchange information. Equal cost path next hops are on two spokes off the same hub. Hubs are configured with "**no ip next-hop-self eigrp.**"

Workaround: Is to clear EIGRP neighbor on spoke that has stale next hop.

- CSCtd89787

  High CPU under interrupt with a large number of alignment errors.

  This condition are seen when issuing **show ip bgp ipv4 mdt vrf <*VRF name*> neighbors**.

  Workaround: None

- CSCtd89963

  Cisco IOS BGP session is flapped on the Cisco ASR 1000 Router Series.

  When the Cisco ASR 1000 Router received BGP UPDATE messages from its peer with invalid AS4_PATH attribute, BGP session is reset and NOTIFICATION message is sent out with error 'update malformed'.

  The symptom is observed only when using the testtool (routem) to generate BGP UPDATE message with mismatched AS_PATH and AS4_PATH attributes to send to the router.

  Workaround: There is no known workaround.

- CSCtd90979

  When configuring hierachical QoS policy-map with precent based rate configuration, the rate calcultion might be wrong when the QoS policy is applied to 10 GigabitEthernet interface.

  The translation from percent to absolute value (in Kbps) might be wrong when QoS policy is applied to 10 GigabitEthernet interface.

  Workaround: To change from using the percent rate to the absolute rate in BPS (bits per second0 in parent shaper would avoid running into this issue.

- CSCte02973

  Routing protocols like EIGRP may be dropped in the global table.

  The symptom is observed when multicast is configured for a VRF and no multicast is configured for the global table.

  Workaround: Is to enable **"ip multicast routing"** and create a loopback interface with **"ip pim sparse-mode"** enabled.

  Further Problem Description: The problem should not occur for MVPN since this is not a valid configuration, as multicast in the core is a requirement.

- CSCte03142

  Enhancement to allow user to configure MAC address for ATM p2p sub-interface.

  To be used for RBE when configuring MAC on that ATM p2p subinterface.

  Workaround: None

- CSCte09171

  When configuring the hardware SIP OIR, we see more v4 and v6 unicast loss than expected on the ASR 1000 Router Series.

  This condition may occur when packet loss has been seen during SIP OIR Test conditions.

Workaround: There is no known workaround.

- CSCte20171

  HSRP active router send ICMP redirect message that source address set to physical interface IP address.

  This condition are observed when Virtual IP address should be used as source address.

  Workaround: There is no known workaround.

- CSCte26324

  Hidden command "l2tp tunnel busy timeout 0" cannot be configured on the ASR 1000 Router Series.

  Workaround: None

- CSCte29212

  1. EIGRP summary-address with leak-map configuration is removed after reloading the router.
  2. summary "leak-map" option is only selectable after entering admin dist.
  3. summaries with the same subnet but different masks overwrite each other.

  The following conditions are seen:

  #1 & #2. EIGRP summary-address is configured with the default administrative distance and a leak-map.

  #3. The same subnet is specified on multiple EIGRP summary-address commands using different masks.

  Workarounds: #1 & #2. Use a non-default administrative distance for the summary route: ip summary-address eigrp 1 192.168.0.0 255.255.0.0 4 leak-map leak-routes #3. There is no workaround.

- CSCte38945

  Unable to get ping reply from the multicast group configured on loopback interface.

  The symptom can occur when there are multiple routes populated in an interface and the interface goes down. All the routers associated with the interface should be removed, but only one is deleted. This results in the ping failure.

  Workaround: Shut down the other interfaces associated with the router and enable it again.

- CSCte39004

  Traceback seen on Pe2 when ipv6 route on ce2 is removed after ipv6 network is removed on pe2 in 6pe fp environment.

  This condition are only seen with IPV6 and MPLS configuration.

  Workaround: None

- CSCte46020

  When using a nas-port-format which is different from default encoding 4/1/3, the NAS-Port-ID and NAS-Port radius attributes do not reflect the requested encoding. This is for sessions which originate on ATM interfaces only, i.e. PPPoEoA.

  Depending on physical interface location, the NAS-Port-ID and NAS-Port radius attributes may not be represented correctly.

  Workaround: Physically move (if possible) the interfaces into ports which can be correctly

  encoded with 4/1/3 bit distribution.

- CSCte50144

A Cisco ASR1002 Router reports incorrect CPU utilization. It reports a low CPU utilisation and also reports an overall utilization lower then the utilization under interrupts.

As shown in this example:

CPU utilization for five seconds: 5%/25%; one minute: 8%; five minutes: 8%

This symptom has been observed on the ASR1002 Router under high CPU utilisation of the RP CPU, caused by excessive rate of punted traffic.

- CSCte50206

  Suppress authentication null-username suppresses system accounting messages

  If you configure 'aaa authentication suppress null-username', system accounting records will not be generated.

  Workaround: None

- CSCte51436

  Symptom: Pressing Hold during a SIP-to-SIP call through CUBE(Ent) on the ASR 1000 Router results in intermittent disconnects. The phone behind the ASR CUBE hears a fast busy tone.

  When CUBE dial-peers are configured with dtmf-relay of: **"rtp-nte"**, **"sip-notify rtp-nte",** or none.

  ASR CUBE(Ent) version from CCO: asr1000rp2-adventerprisek9.02.05.00.122-33.XNE.bin

  Workaround: Is to use **"sip-notify"** as the dtmf-relay method.

- CSCte51715

  Logs will appear with the following error message:

  %IOSXE-4-PLATFORM: R0/0: kernel: EXT2-fs warning: checktime reached, running e2fsck is recommended

  In this condition there is no service impact on the router, only logs are generated frequently.

  When a Cisco ASR 1000 Router is running any image before 12.2(33)XNF1 release.

  The images for 12.2(33)XNF1 has the fix for this condition.

  Workaround: Is to perform the following steps:

  1. 1. Drop into Linux shell
  2. 2. Issue the following set of commands:

  /sbin/tune2fs -c 0 -i 0 /dev/sda1

  /sbin/tune2fs -c 0 -i 0 /dev/sda2

  /sbin/tune2fs -c 0 -i 0 /dev/sdb1

  /sbin/tune2fs -c 0 -i 0 /dev/sdb2

- CSCte52369

  On a Cisco ASR1000 Router, the RADIUS will send a NACK for the first COA request message and Radius Authentication will fail.

  This condition are seen when the RADIUS recieves "ACCESS-ACCEPT" with 'Unsupported Vendor' attribute

  Workaround: Work around is to send the COA request message again.

- CSCte53365

The connected EIGRP-owned global addresses are put into the EIGRP topology database after the IPv6 router eigrp <as> process is configured to **"no shutdown".**

This symptom is observed when the router is reloaded with an IPv6 EIGRP instance configured **"shutdown"**, then the configuration is changed to **"no shutdown"**.

Workaround: Configure **"shutdown"** then **"no shutdown"** on the interfaces.

- CSCte58468

  OSPF process running in global routing table does not declare it self as ASBR router in the router LSA (E-bit is not set) and therefore his external default route is not installed.

  This problem happens during reconfiguration after 'router ospf X' is removed from the configuration and later added back.

  This problem are seen only if another OSPF process which runs in VRF is configured, but not always. Both processes must share internal datastructures.

  Workaround: None

- CSCte58825

  There is a crash upon conducting an snmpwalk from "enterprise mib oid 1.3.6.1.4.1".

  The symptom is observed on a Cisco ASR 1000 Series Aggregation Services router that is running Cisco IOS Release 12.2(33)XNE.

  Workaround: Configure SNMP view to exclude ipSecPolMap as follows:

  snmp-server view <view name> iso included

  snmp-server view <view name> ipSecPolMapTable excluded

- CSCte60167

  EIGRP IPv6 is no longer active on an interface.

  This condition has been observed after removing HSRPv6 configuration from the interface.

  Workaround: Is to do **shutdown** and **no shutdown** on the interface.

- CSCte62914

  Track process timer is scheduled 1000 per second because there is no default timer value for track stub object. There are no known serious side effects, although the extra schedules could degrade performance by a small amount when system is under load.

  If track ***<number>*** stub object is configured, then a timer is started using 0 as the timer frequency which results in a 1 millisecond timer.

  Workaround: Do not use stub object tracking.

- CSCte64090

  After Route Processor (RP) switchover, PPPoE traffic may drop though sessions that will stay up.

  This condition has been seen when triggering a Route Process (RP) switchover via command **redundancy force-switchover**.

  Workaround: None

- CSCte64156

  Under certain circumstances, the ROMMON variables may show: "PLATFORM_MAX_INTERFACES =128K" while there is no "platform max-interface 128k" configured.

  This usually occurs after the router has been reloaded.

Workaround: Is to configure “platform max-interface 128k” and then “no platform max-interface 128k”. A reboot is recommended after.

- CSCte69014

  Multiple memory leaks are seen when you try to bring up an unauthenticated session:

  0x11FF95E0 7812 37 AAA Request Data

  0x11FFA020 4692 18 SSS AAA auth req

  0x11CBD48C 1692 18 AAA AUTHEN Username

  The symptom is observed when a TAL authorization failure occurs due to access-reject. When you try to bring the session up again this leak is seen.

  The following steps are:

  1. Configure L2-connected session.
  2. Bring up an L2-connected IP session and verify the access-reject event is triggered.

  3. Check for these leaks using ""show memory"" commands.

  Workaround: There is no workaround."

- CSCte69621

  Missig CLI for configuring deny policy options:

  crypto ipsec ipv4-deny {clear|deny|jump}

  Workaround: None

- CSCte69761

  Intermittently the eigrp learned default route (0.0.0.0/0) is deleted from the routing table.

  If a router receives a default-network and 0.0.0.0/0 prefix and both are marked as candidate default prefixes in the routing table, and the default-network prefix is lost/deleted, the 0.0.0.0/0 prefix will also be deleted from the routing table even though an EIGRP topology entry remains for the 0.0.0.0/0 prefix.

  Workaround: Is to do the following:

  1. A **clear ip route *** can be issued and the EIGRP topology table entry for 0.0.0.0/0 be re-installed again into the routing table.
  2. Configure ‘no default-information in’ under the router EIGRP process on the router which intermittently loses the 0.0.0.0/0 prefix.
  3. Reconfigure the network, if possible, to discontinue use of the ‘ip default-network’ command and rely on the use of the 0.0.0.0/0 prefix.

- CSCte72075

  BGP VRF IPv6 session fails to stay up. As soon as a BGP End-Of-RIB (EOR) message is send the peer responds with an update malformed BGP notification and the session is torn down. The session gets stuck in NoNeg state.

  This condition Two BGP routers each configured with a VRF that attempt to establish an IPv6 BGP session within the VRF.

  Workaround: There is no workaround.

- CSCte72128

  After reload, ""cdp enable"" is missing on tunnel interfaces.

  The following conditions have been observed:

  - Having CDP actiavted on tunnel interfaces (for ODR usage in DMVPN for example)
  - Running XNE1, this has not been seen on 12.2(33)XNE

  Workaround: Is to add it manually, after a reload.

- CSCte73093

  EIGRP resync is not triggered when modifying inbound with outbound prefix-list or ACL.

  This condition has been observed when there is an interface associate with EIGRP distribute-list .

  Workaround: Use distribute-list without any associating interface.

- CSCte75406

  A crash can occur if the memory is low during the initialization of the OSPF process.

  The symptom is observed if the memory is low during OSPF process initialization.

  Workaround: There is no workaround."

- CSCte75784

  About 500 bytes of memory is leaked for each configured delegate subscriber that has the supported options header configured for it. The memory is lost during each show with run or wr mem.

  This condition are seen when configuring the delegate subscriber with the supported options header tags.

  Workaround: Do not configure supported options header tags.

- CSCte77136

  CLNS routing over GRE tunnels is not working on the ASR1000 Router.

  Conditions: CLNS routing over GRE tunnels is configured, specifically with a GRE tunnel as the egress interface (output from the ASR100). In this scenario, CLNS packets are not forwarded via fast switching.

  Workaround: I to use the following configuration change (needed on a per interface basis):

  “no clns route-cache” “to disable CLNS fast switching”

- CSCte78165

  On the Cisco ASR 1000 Router a device may reload when the 'show ip protocol' is issued.

  This condition may occur when the Routing protocol is configured, and is trying to redistribute ISIS routes.

  Workaround: Do not use the **show ip protocol** command for now.

- CSCte79759

  On a DMVPN hub router, NHRP multicast replication entry is not deleted from its replication list when the corresponding nhrp cache entry is deleted.

  This problem occurs when a DMVPN spoke is no longer registered with a DMVPN hub router.

  Workaround: The workaround is to remove the tunnel interface on the DMVPN hub router and re-add it.

- CSCte83888

  When PoD request contains target Acct-Session-Id prepended with NAS-Port-ID it will not be honored.

  This condition are seen when PoD prepended with NAS-Port-Id for target session.

Workaround: Is to use only the Session-Id which is located after the, "_" in the Account-Session-ID to specify the session needing disconnect.

- CSCte89787

  A Cisco ASR 1000 Router crashes after the Segment Switch Manager (SSM) reports that an invalid segment has been detected:

  %SW_MGR-3-INVALID_SEGMENT: Segment Switch Manager Error - Invalid segment - no

  segment class.

  The crash follows this message.

  The symptom is observed on a Cisco ASR 1002 that is running Cisco IOS Release 12.2(33)XND1. The crash is caused by a NULL pointer de-reference following the "no segment class" error. The error itself is not fatal and the crash should have been avoided.

  Workaround: There is no workaround.

- CSCte92659

  On the ASR 1000 Router Series show memory debug leaks would show SSS holding some memory.

  This condition are seen during longer hours of session flapping.

  Workaround:None

- CSCte92745

  After removing a user in resource policy the Cisco ASR 1000 Router fails in the first attempt.

  This conditon are seen only with the first attempt and second time gets removed.

  Workaround: None

- CSCte92790

  Router has unnecessary periodic (50mins) BGP update without topology change.

  This condition are seen when configuring BGP Best External feature on EDGE router as ""bgp advertise-best-external"".

  Workaround: None

- CSCte94156

  When running Release 2.5.1 the Cisco ASR 1000 Router fails to update the PST value in TBAR., causing other

  GM to fail sending traffic on the ASR 1000 Router with anti-replay error messages. This happens whenever the local ACL is changed on the GM or by KS failure and recovery.

  Workaround: None

- CSCte94237

  A crash happened when type cli **sh sbc <*non-exist sbc name*> sbe sip statistic** ASR 1004-2#sh sbc afaf sbe sip statistics SBC “afaf” has not been configured.

  No SIP statistics found.

  ASR1004-2#

  *Feb 10 10:34:40.228 SGT: %SCHED-2-SEMNOTLOCKED: Virtual Exec attempted to unlock an unlocked semaphore -Traceback= 1#359fd7114b043d9cc307b84aa384d228 :10000000+B95EA0 :10000000+B96224 :10000000+20BDEA4 :10000000+34E3578 :10000000+359D3B4 :10000000+359EF50 :10000000+B02D30 :10000000+B0954C :10000000+283AF14 :10000000+B1766C

This will limit the memory address space engine can use to 3400MB, thus limiting the call in progress.

This condition are seen when typing cli ""sh sbc <non-exist sbc name> sbe sip statistic"" in console.

Workaround: Is to only type that command with a configured sbc name.

- CSCte97907

  On a Cisco ASR 1000 Router with 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: None

- CSCte98082

  PPPoE Relay Session is failing to come up on LAC with some specific configuration.

  Workaround: None

- CSCtf00427

  A router may experience a severe memory leak issue when the following command is configured:

  privilege exec level <*level*> show ip

  ospf neighbor

  The symptom is observed when running Cisco IOS Release 12.2(33)XNE

  or 12.2(33)XNE1. The issue is not platform dependent.

  Workaround: Is to reload the router.

- CSCtf01344

  IOSD core@chunk_diagnose while doing ASR 1004 ISSU upgrade.

  The problem is limited to the 4RU when attempting an ISSU upgrade with VRF-aware IPSec features and an uninitialized webex SPA in the system.

  Workaround: Properly initialize Webex SPA before ISSU upgrade.

- CSCtf05183

  Tracebacks are seen when changing tunnel mode from gre or ipip to ipsec ipv4 with cdp enabled.

  This problem are seen when changing tunnel mode from gre or ipip to ipsec ipv4 with cdp enabled.

  Workaround: None

- CSCtf07776

  The below traceback can be seen in two scenarios on a Cisco ASR 1000 Router:

  - During UUT reload
  - After shutting the FRR enabled interface

  ```
  %FRR_OCE-3-GENERAL: un-matched frr_cutover_cnt.
  -Traceback= 40DCB368 40DCB220 40DCB444 40DEC968 40D15FE4 40D1BACC 40D13BD4 40D14810
  ```

  This condition are seen on the router with TE and FRR enabled on interface during the reboot and issue.

  Workaround: There is no know workaround.

  Further Problem Description: This problem has no impact on forwarding functionalities, but it does have performance impact on unstable network situations.

- CSCtf07907

  RP Crash observed when doing RP switchover after deleting some tunnel configuration.

  This instance may occur when switchover is to be done after deleting some tunnel config and traffic is flowing in background.

  Workaround: None

- CSCtf11997

  For the following sbc-sbe configuration:

```
call-policy-set 1
irst-call-routing-table RT-DSTADDR
rtg-dst-address-table RT-DSTADDR
entry 1
match-address ^bus[0-9][a-z] regex
```

  The command “no match-address” would NOT delete (i.e. unconfig) the match-address.

  This is also observed for the match-address under rtg-src-address-table configuration.

  Workaround: The workaround is to delete “entry 1” or “rtg-dst-address-table RT-DSTADDR” or “call-policy-set 1”.

- CSCtf15848

  The following error seen on re-configuring channel-groups after switchover

  EFC ERROR: spa_efc_config_ds1_channel - channel in use

  The following conditions have been seen:

  - active RP booted with 8xcht1/e1 and channel-group is configured on t1 controller
  - load the standby RP, and do a switchover
  - on new active RP, unconfigure and reconfigure the channel-group

  Tracebacks with “EFC ERROR: spa_efc_config_ds1_channel -channel in use” seen.

  Workaround: before switchover, configure channel-groups on active RP when standby RP is up.

- CSCtf16359

  The ASR 1000 Router when configured as GETVPN GM will not make any local GM acl change of removing extended ACL effective, until a new rekey from Key server has been configured.

  This condition has been seen when the ASR 1000 router is configured as GETVPN GM.

  Workaround: None

- CSCtf17273

  A Cisco ASR 1000 Router crashes during startup when receiving an AS_SET attribute from its peer.

  This symptom is observed when the BGP peer sends an AS_PATH or AS4_PATH containing an AS_SET attribute.

  Workaround: There is no workaround.

- CSCtf19923

  IP SLA: icmp-echo detect 300+ msec delay on a Cisco ASR 1000 Router.

  This has been seen under corner conditions an incoming packet might be delayed by about 900 msec resulting in incorrect IP SLA. This is the max delay if there are no other packets received after the icmp response occurrence is very rare about 2 to 3 times in 10,000,000 pkts

  Workaround: None

- CSCtf21390

  When EIGRP for IPv6 is used and a default route summary is entered on an interface (::/0), the appropriate topology table entry and IPv6 route is not created or sent to peers. This conditions are seen when default route summary is entered on an interface (::/0) in EIGRP for IPv6.

  Workaround: Is to use a summary other than ::/0, since other summaries beside the default route work correctly.

- CSCtf25514

  Policy routing is enabled on Virtual Template interface when ip policy route-map command is downloaded via Radius, while it is not supported via CLI.

  Above symptom is seen on Cisco ASR 1000 Routers running IOS of version 122(33)XND, 122(33)XNE and 122(33)XNF.

  Workaround: None

- CSCtf26943

  Session is not going down after per-user push on a Cisco ASR 1000 Router.

  This condition happens after a Per-User Push from RSIM with incorrect QoS attributes Session is not going down.

  Workaround: None"

- CSCtf26946

  The ASR 1000 Router crashed when mis-input command **no int sbc1** under ASR1004-3(config-sbc-dbe)#

  The conditions are seen when the following has occurred:

  1. provision sbc1 interface
  2. provision dbe and media-address
  3. input **no interface sbc1** under ASR1004-3(config-sbc-dbe)#

  Workaround: None

- CSCtf32412

  Tunnel drops [Phase I and Phase II's] may occur on the ASR 1000 Router.

  If a specific phase II pair of SA's is timing out due to configured idle time, then the

  ASR 1000 Router will drop the Phase I, all Phase II to that particular peer and create a tunnel drop.

  Workaround: Do not use crypto ipsec security-association idle-time.

- CSCtf32693

  On Cisco ASR 1000 Router, configuring xconnect on a VLAN, SNMP 64 bit counters are not getting updated.

  This condition are seen when one of the vlan on same port have xconnect configuration.

  Workaround: There is no workaround.

- CSCtf33363

  Port information is missing in nas-port string sent to Radius on the ASR 1000 Router Series. This instance may occur with PPP sessions on the router.

  Workarounds: None

- CSCtf33960

Router alart label 1 is deleted upon SSO, so mpls ping over and RA only PW failed.

This issue has been observed in RA only l2vpn configuration.

Workaround: None

- CSCtf36402

  The ASR 1000 Router may crash when the user telnets and Transmission Control Block is cleared for that session before entering password. This instance has been observed when AAA Authentication protocol is set to TACACS.

  Workaround: Do not clear the Transmission Control Block for a session before entering password.

- CSCtf40702

  A Cisco ASR 1000 Router Series with Route Processor 2 Engine may unexpectedly reload do to a SegV crash. This will happen if there is a monitor session configured that uses a source interface with a range. This can either be a crash while configuring via cli or a crash at bootup if the command is in the startup configuring.

  Workaround: Don not use the source inter range

  CSCtf41171

  With QoS policy accounting enabled, using the **clear subscriber session uid <*uid*>** command to clear a session can result with incorrect packet/byte counts on the generated accounting Stop record.

  The following conditions are seen:

  1. QOS accounting enabled
  2. The SAME accounting group is applied to a class in BOTH the input AND the output policy-maps.
  3. **clear subscriber session uid <*uid*>** is used to clear the session

  Under these conditions the packet/byte counts on the generated accounting Stop record may be incorrect.

  Workaround: Is to use an alternate method to clear the session, such as **clear pppoe all** or **clear ppp interface <*interface*>**.

- CSCtf54092

  Wrong if index exported to NFC log when polling for ATM sub-interface.

  This condition has been seen when ATM sub-interface is configured.

  Workaround: None

- CSCtf59446

  On a Cisco ASR 1000 Router the Standby Router processor may experience a s/w reset.

  This condition has been seen when the ASR 1000 Standby Router processor experiences a s/w reset, after issuing "**show l2tp session interworking username <username>"** on the standby route processor while L2TP tunnels are establishing.

  Workaround: Is to issue the command **"show l2tp session interworking username <username>"** in active route processor to get command output without any s/w reset.

- CSCtf59781

  When DHCPv4 client sends dhcp discover packet with broadcast flag = off, the performance of Cisco ASR 1000 Router working as DHCPv4 relay is not good compared to if it receives dhcp discover packets from client with broadcast flag = on.

This problem is expected only if the dhcp client is sending discover packet with broadcast flag = off(unicast).

Workaround: None

- CSCtf66271

  An ASR 1000 Router running asr1000rp1-adventerprisek9.02.04.02.122-33.XND2.bin, upgraded to asr1000rp1-adventerprisek9.02.06.00.122-33.XNF.bin displays the complete cert chain like:

```
crypto pki certificate chain JUTnetRoot-Pilot
certificate ca 3C5A00179190F2DF23325330195B9B67
308203AE 30820296 A0030201 0202103C 5A001791 90F2DF23 32533019 5B9B6730
0D06092A 864886F7 0D010105 05003071 310B3009 06035504 06130255 53311930
17060355 040A1410 41542654 20436F72 706F7261 74696F6E 311F301D 06035504
0B131646 6F722054 65737420 50757270 6F736573 204F6E6C
:
:
truncated
```

  Whereas before upgrade it displayed the same as:

```
crypto pki certificate chain JUTnetRoot-Pilot
certificate ca 3C5A00179190F2DF23325330195B9B67 nvram:ATTCorporati#9B67CA.cer
```

  This condition has been seen when ASR 1006 running asr1000rp1-adventerprisek9.02.06.00.122-33.XNF.bin image.

  Workaround: None

- CSCtf85471

  Tunnel Client Auth-ID mismatch has been seen between the Active and Standby RP when load-balancing profile is used with Radius.

  Issue is seen with specific RADIUS profile for load-balancing.

  Workaround: The workaround is to disable load-balancing.

- CSCtf91603

  In a CUBE(SP Edition) ASR 1000 system configured for H.323 video calls, in some instances where the endpoints send large H.323 TCS messages a video call may be connected with only audio or fail to setup the call entirely.

  This condition may occur when TCS message must be large.

  Workaround: Is to configure H.323 Video endpoints to advertise fewer capabilities.

- CSCtf95205

  The **show sbc global dbe signaling-flow-stats** reports incorrect value for “Reserved Bandwidth” on the termination whose tman/pol is set as “OFF”.

  When the Cisco ASR 1000 Router creates a pinhole based on the received MEGACO ADD request which sets tman/pol=ON with tman/sdr&tman/mbs parameters for one side termination and tman/pol=OFF without tman/sdr&tman/mbs parameters for the other side termination.

  Workaround: None

- CSCtg02140

  Upon switchover with the webex call flow, media is not preserved.

This problem has been seen when switchover with webex flow Add(A,B), Delete (B), and Add (A,C) has been used.

Workaround: None

- CSCtg02617

  The following error has been observed on the ASR 1000 Router console:

  Config Sync: Line-by-Line sync verifying failure

  The above error has been seen when entering any parser CLI in parser view on the router.

  Workaround: None

- CSCtg06681

  SIP method profile allows defining a mapping of status-codes. RP2 CUBE(SP Edition) would crash while removing status-code map.

  For RP2 CUBE(SP Edition), consider the following configuration:

```
config t
sbc test
sbe
sip method-profile SIPmessage
method INVITE
action as-profile
map-status-code
range 183 value 180     <==== incorrect mapping
end
```

Note That there is only one entry for mapping status-code.

When we try to unconfigure “range 183 value 180” as follows the RP2 CUBE(SP Edition) would crash:

```
config t
sbc test
sbe
sip method-profile SIPmessage
method INVITE
map-status-code
no range 183 value 180  <=== causes crash
end
```

Workaround: The workaround is to unconfigure “map-status-code” and then re-configure it with correct mapping of status-code as follows:

```
config t
sbc test
sbe
sip method-profile SIPmessage
method INVITE
no map-status-code   <==== unconfigure map-status-code
map-status-code         <==== re-configure
range 180 value 183   <==== correct mapping
end
```

- CSCtg11844

  Crypto tunnel will not come up and pass traffic on the ASR 1000 Router Series. This condition are seen when the ASR 1000 Router running IOS 12.2(33)XNF code with nat outside and a crypto map on the same interface, if you remove and readd the crypto map from the nat outside interface the

crypto tunnel will not come up and start passing traffic until such time as you remove the ""ip nat outside"" statement. Once the crypto map is up and running you can readd the ""ip nat outside"" command.

Workaround: Is to remove the nat outside command, get the crypto tunnel up and passing traffic then readd the nat outside command back to the interface.

- CSCtg17977

  BBA L2TP LNS subscriber sessions are not in sync between Active and Standby RP's. This condition has been observed during ISSU upgrade.

  Workaround: There is no known workaround.

- CSCtg27141

  UDP Jitter operation is not working on the ASR 1000 Router Series.

  This condition has been when using UDP Jitter the operation is not working after time out failure occurs on the router.

  Workaround: None

Open Caveats—Cisco IOS XE Release 2.6.0

This section documents possible unexpected behavior by Cisco IOS XE Release 2.6.0

- CSCsw78270

  SIP core during ISSU has been observed intermittently, when upgrading, or downgrading to 2.3.0 Release.

  This instance may only occur, while executing ISSU runversion on the 6RU, 4RU and 2RU superpackages after upgrading from 2.2.0 to 2.3.0 releases.

  Workaround: None

- CSCta24676

  On the ASR 1000 Router when an attempt is made to login to the kerberos client, the RP crashes. This is after the clocks of the UUTs are synchronized and the routers are configured with kerberos credentials.

- CSCta46670

  When disabling and enabling **control plane host** a few times this may generate an error message on the Cisco ASR 1000 Router. This has been observed, when configuring **control plane host** followed by **no control plane host** a few times on the router.

  Workaround: None is required since there appears to be no functional impact.

- 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: None

- CSCtb98877

  On the ASR 1000 Router Series subsequent call fails after a SIP Session Refresh timeout occurs after an HA switchover in CUBE environment.

  This occurs in a back to back CUBE environment:

CUCM1 - SIP - CUBE1 - SIP - CUBE2 - SIP - CUCM2

The CUCM SIP Refresh is set to 90 seconds, and a call is made. HA switchover occurs on CUBE1, and the call is disconnected as expected.

The same call is made again, but the originating endpoint on CUCM1 gets a Busy tone, while the terminating endpoint on CUCM2 gets Ringing tone.

CUBE2 sends a 503 Internal error with the following cause code:

Reason: Q.850;cause=38 - [Network out of order]

Workaround: None

- CSCtc13911

  Backup tunnels in TE FRR scenario keeps flapping after RP reload.

  This may happen only with MIB walk through in tandem.

  Workaround: To Do an RP switchover. Without this workaround it takes 2 to 3 hours for the tunnels to become stable.

- CSCtc35744

  Configure a user profile with multiple 'Cisco-Avpair=lcp:interface-config=<*cmd*>'. Create pppoe session. The per-user access-list attributes get downloaded from the AAA server, and the attributes are applied. The show subscriber session detailed output shows that only the first 'Cisco-Avpair=lcp:interface-config=<*cmd*>' is getting applied on the session. Typical features configured on a PPP Virtual Access on a per-users basis using this vsa would be IPUnnumbered, VRF, Keepalive, Pool name, PBR, multicastjoins, etc.

  This issue is seen when a PPPoE session is brought up with a user profile that has more than one 'Cisco-Avpair=lcp:interface-config=<*cmd*>'configured.

  Workaround: The workaround is to configure multiple Cisco-Avpairs in 1 line.

  For example:

  Cisco-AVPair = **lcp:interface-config=ip vrf forwarding vpngreen**

  Cisco-AVPair = **lcp:interface-config=ip unnumbered loopback2**

  Should be configured like this:

  Cisco-AVPair = **lcp:interface-config=ip vrf forwarding vpngreen \nip unnumbered loopback2**

- CSCtc44482

  When deleting VRF while STANDBY RP comes up, when SSO switchover happens this may cause an error message after STANDBY RP has been reloaded.

  The following error message has been seen:

  SYS-3-HARIKARI

  Workaround: Do not delete VRF prior to STANBY RP achieving the STANDBY HOT state.

- CSCtc54288

  When changing the group number associated with a virtual IP address causes hosts to lose contact with the virtual router.

  This instance occurs when a virtual IP address is associated with one group, and then that group is unconfigured and the same virtual address used by another group. Since each group is uniquely associated with a virtual MAC address the ARP tables of all hosts that were using the previous group

will contain invalid entries. When the interface is shut, while configuring new groups then gratuitous ARPs will be sent to refresh any hosts' ARP tables before the interface is ready to forward traffic. The hosts will not realize that the vIP/vMAC association in their ARP tables are invalid and will be unable to forward traffic via the known (virtual IP) gateway.

Workaround: A delay can be used to stall the VRRP initialization process after unshutting an interface:

vrrp delay minimum

reload

The values used are the number of seconds to delay, which is platform dependent. 30 seconds for interface delay and 300 seconds for reload delay are a good first values to test.

- CSCtc55049

  The ASR 1000 Router may crash 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: None. However if 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.

- CSCtc55215

  On the ASR 1000 Router, when shape rate is configured as % of an ATM PVC for GRE QoS it is not updated after the PVC rate has changed.

  This may occur when changes to the PVC rate and its ATM class has been configured on the router at the same time.

  Workaround: None

- CSCtc58124

  When traffic is flowing, (S,G) expiry timer should be updated to 3:30 seconds every 2 minutes. In the VRF context, the expiry timer on (*,G) and OIF is updated but on (S,G) is not on the ASR 1000 Router Series. This will work fine in the Global Context on the router.

  This happens, when **vrf** is configured on router.

  Workaround: There is no workaround.

- CSCtc62440

  On a Cisco ASR 1000 Router Series, the removal of sub-interfaces 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.

- CSCtc67457

  On the RP2 a crash has been seen with process IKMP.

  This has been observed, when GetVPN Group Member is configured with vrf-lite on the RP2.

  Workaround: No known workaround.

- CSCtc69297

Tracebacks has been seen with cli **sh platform hardware qfp active feature acl tree** on the Cisco ASR 1000 Router.

This condition has been seen, when there are a huge number of acls configured on the router.

Workaround: None

- CSCtc70742

  ASRNAT allows removal (unconfiguration) of static entry even when entries has children translations.

  Workaround: There is no known workaround.

- CSCtc78745

  When deleting a few tunnels from PE side, when CE and PE are having different number of tunnels the Cisco ASR 1000 Router starts throwing msgs.

  The following message has been seen:

  ```
  Oct 27 14:33:40.170 IST: %ACE-3-TRANSERR: ASR1000-ESP(14): IKEA trans 0x1D8C; opcode
  0x60; param 0x1FD2; error 0xA; retry cnt 0
  ```

  This condition has been observed, when tunnel mismatch between CE and PE are kept for a long time on the router.

  Workaround: The are no known workaround as of now.

- CSCtc86866

  While unconfiguring IP NHRP, when mapping has been given a different NBMA Address this clears the original address on the ASR 1000 Router Series.

  Workaround: None

- CSCtc91018

  On a Cisco ASR 1000 Router the subinterface counters with Frame Relay Encapsulation can show higher values than the counters on the main interface, when self-pinging the subinterface.

  Workaround: None

- CSCtc96467

  STANDBY RP reloads twice with **issu runversion**, while downgrading from Release 2.6 to 2.5.

  This instance may occur, when Super Package has been configured with ISSU, which causes the STANDBY RP to reload with **issu runversion**.

  Workaround: None

- CSCtd00489

  A traceback indicating that the object was being deleted before the ideal exponent is invalidated has been logged on the ASR 1000 Router Series. An schedule object is freed before the ideal exponent is invalidated. This condition is treated as an error because this points to a missing step in cleaning up prior to destroying an object since this can potentially impact the rate accuracy in the future. This issue occurs while an ATM VC schedule is being deleted on the router.

  Workaround: There is no known workaround. There is also no negative side effects identified in the systems where this issue has occurred. The system will continue to operate normally.

- CSCtd03743

  Ping fails when VFR is removed on the Cisco ASR 1000 Router.

  This instance has been observed after removing the VFR, when trying to ping the destination router loopback with larger packet size, then the ping fails on the router.

Workaround: To ping with small packet size of 3000 and 1500 on the router. Do not ping with packet size of 9300 this will cause the router to fail.

- 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: None

- CSCtd22958

  With basic SIP calls RTP traffic running (20 CPS, 1200 sustained calls), a physical OIR of ESP, -25% of active call media traffic is lost for a 20-30 second time period and signaling for new calls coming into Unified SBC during this time period are rejected with 500 - Server Internal Error.

  Workaround: Avoid physically removal of active ESP, when Unified SBC calls are in session. To use soft OIR instead.

- CSCtd36301

  At every session churning of IPv6 PPPoE uses more prefixes for same tunnel and session value.

  No used IPv6 Prefixes in local IPv6 pool are incremented at every session flap iteration in IPv6 LNS for same tunnel and session value.

  This instance may happen, when Local IPv6 prefix pool is used to assign ipv6 address and the sessions are churning at a flap rate of 70 sessions per seconds for 8000 sessions.

  Workaround: None

- CSCtd37057

  On a heavily loaded Cisco ASR 1000 Router Series, rapid QoS queuing configuration changes involving the removal of existing configuration and addition of new configuration could cause the system to experience temporary resource outage. The conditions under which this has been observed involve 32000 flapping PPPoE sessions combined with configuration changes on the system.

  Workaround: Avoiding rapid and large QoS configuration changes on a heavily loaded system will avoid the problem reported in this caveat.

- CSCtd48042

  When defining vrfa adjacency the vrfb as singal-address is used, this can start an attack and the EP will show in vrfa blacklist on the Cisco ASR 1000 Router.

  This instance may occur, when vrfa adjacency has been defined, but vrfb as singal-address is used on the router.

  Workaround: None

- CSCtd48500

  SNMP 64 bit counters not showing traffic. This has seen seen on ASR1002 running 12.2(33)XND1 and XND2 after deploying an AToM Circuit under it.

  Workaround: None

- CSCtd49186

  After the Cisco ASR 1000 Router has been reloaded this removes saved VASI, Subinterface, Loopback Interface CLIs under Parser View.

  This condition has been observed, when accessing parser view for saved interfaces followed by a reload on the router the interfaces were removed.

Workaround: After reload all of saved interface configurations will need to be re-configure under each parser view on the router.

- CSCtd62358

  On a Cisco ASR 1000 Router Series, the rapid deletion and re-creation of VASI interfaces may result in failures in the functioning of the VASI interfaces.

  Unexpected resets of the ESP have also been observed under these conditions.

  Workaround: Delaying of the order of 2 minutes between the deletion and re-creation of VASI interfaces will avoid this problem.

- CSCtd64206

  FP crash may occur, when ISG DHCP sessions flap has churned on the Cisco ASR 1000 Router.

  This condition has been oberved in ISG DHCP stressed environment.

  Workaround: Is to lower the scale of both number of sessions and session churn rate.

- CSCtd70901

  During RP switchover, a Cisco ASR 1000 Router running 2.6.0 release may experience IPv6 multicast channel zapping latency more than expected.

  This condition has been seen, when RP failover from the active to the standby has occurred.

  Workaround: There is no known workaround.

- CSCtd80542

  Loop observed, when configuring SNMP bulk mib walk. The loop has been observed at tunnelInetConfigIfIndex.

  This condition has occurred, when scaled configuration includes tunnel interface 2147483647.

  Workaround: None

- CSCtd84323

  Under Unified SBC SIP IPv6 to IPv4 scenario with DTMF digits via INFO method, the following Traceback has been seen on the console following RP failover scenario:

  ```
  "*Dec 14 20:59:14.494: %ASR1000_INFRA-5-IOS_INTR_HISTORY: [5|0] [0:0] [0->0] ra[ 1* 0x0 1* 0x0 ] -Process= "SBC main process", ipl= 0, pid= 314".   The traceback causes a temporary outage in service, but SBC does recover without any manual intervention.
  ```

  This traceback has been observed in the following conditions:

  1. SIP IPv6 to IPv4 calls
  2. DTMF digits transferred via INFO method
  3. RP failover has been executed at some point in past.

  Workaround: None

- CSCtd87072

  IOSD will restart, when changing tunneling mode in scaled IPSec Sessions on the ASR 1000 Router Series.

  This condition has been observed, after IOSD restarts the tunneling mode has changed in a scaled IPSec Session enviroment.

  Workaround: None

- CSCtd87205

  The Cisco ASR 1000 Router will reload, when flapping up and down VC's after configuring SSO.

This condition has been observed, when the Cisco ASR 1000 Router reloads after a large amounts of flapping has occurred, and SSO has been forced onto the router. The router may reload.

Workaround: Is to slow down the amount of flapping when doing SSO on the router..

- CSCtd90836

  During REKEY there are a lifetime of IPSEC sessions that show junk characters on the ASR 1000 Router Series.

  This conditions has been observed, during rekey.

  Workaround: None

- CSCtd91015

  The Cisco ASR 1000 Router does not roll back to the base image even though the rollback timer has expired for ISSU Superpackage Downgrade from Release 2.6 to 2.5. ISSU Superpackage Downgrade does not finish within the specified “roll back” time, but router does not rollback to the base image. Tracelogs shows that the timer has been expired and a user prompt has appeared. But the prompt does not appear on the console. SPA's will move to “inserted” mode and at certain times STANDBY RP will reload.

  Workaround: ISSU will work fine, when rollback time is increased.

- CSCtd91950

  A Cisco ASR 1000 Router Series with the Lawful Intercept feature configured may reset unexpectedly under certain conditions when streams are modified/disabled/re-enabled during traffic flow.

  The conditions necessary for this situation to be encountered are multiple MDs, configuration of circuit-id based pre-provisioned stream entries and active PPPoE sessions.

  Workaround: There are no known workarounds.

- CSCtd91986

  Under certain conditions a Cisco ASR 1000 Router Series configured with the Lawful Intercept feature may not intercept traffic sent from a PPPoE client though the packets reach the destination as expected. This may happen when a circuit-id based PPPoE session is up and traffic is sent from the PPPoE client. This may happen for both forwarded and PTA PPPoE session cases.

  Workaround: There are no known workarounds.

- CSCtd98510

  Some of the L2TPv3 Xconnects are not coming up after repeated (5-6) switchovers and OIR.

  This condition has been observed ,when AC is down and session is in local and not ready state.

  Workaround: Is to clear l2tp recovers the problem.

- CSCte01388

  The FMAN FP process may crash on the ASR 1000 Router Series.

  This has been observed, when VPN has been configured on the router.

  Workaround: None

- 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.

- CSCte20171

  HSRP ACTIVE Router sends ICMP redirect message that the source address is set to a physical interface IP address. The Virtual IP address should be used as source address.

  Workaround: None

- CSCte28845

  With Cisco ASR 1000 Router operating in uSBC mode, all adjacencies are locked in Detached state after an upgrade or change where the SBC must be deactivated and activated. When SBC is deactivate or activated or the same for one of the adjacencies, the system prints a routing error log.

  The problem occurs when there is an digit routing entry in the routing table that is missing the destination adjacency datafill.

  In most cases the SBC will not allow this to be configured in the first place without throwing an error but there are some scenarios where this configuration can get into the database without an error.

  Workaround: Remove the entry with “no dest adjacency” or “add a dest adjacency” to the entry datafill.

- CSCte42733

  When configuring ip verify unicast reverse-Path and no ip verify unicast reverse-path in a virtual-template and then applying to a ppp session which causes a FP core dump. This condition has been observed, when URPF has been configured on the ASR 1000 Router.

  Workaround: Is to **enable** and **disable urpf** in the same virtual-template.

- CSCte42926

  Some L2 VPN circuits (PW) are missing or stays down after **clear xconnect all**. This condition has been seen in Scaled L2 VPN environments which includes L2 VPN ATM PWs, EoMPLS and Local Switching.

  Workaround: Is to **reload** the router.

- CSCte43453

  QoS accounting Interim record for the parent policy-map class-default class has incorrect packets and bytes stats while under traffic load. This condition has been seen when PTA session with Model D2.2 QoS has been enabled. QoS accounting has been enabled at the parent policy-map class-default class. While under traffic load, the accounting Interim record has incorrect stats as compared to the QoS stats in the output of **show policy-map session**.

  Workaround: None

- CSCte43891

  When QoS policy accounting has been enabled, using the **clear subscriber session uid <uid>** command to clear a session can result in incorrect packet/byte counts on the generated accounting Stop record.

  This condition has been seen when following has occurred:

  1. **qos accounting enabled**
  2. The SAME accounting group is applied to a class in BOTH the input AND the output policy-maps.
  3. **clear subscriber session uid <uid>** is used to clear the session, under these conditions the packet/byte counts on the generated accounting Stop record may be incorrect.

Workaround: Is to use an alternate method to clear the session, such as **clear pppoe all** or **clear ppp interface <interface>**

- CSCte46020

  When using a nas-port-format which is different from default encoding 4/1/3, the NAS-Port-ID and NAS-Port radius attributes do not reflect the requested encoding. This is for sessions which originate on ATM interfaces only, i.e. PPPoEoA.

  Depending on physical interface location, the NAS-Port-ID and NAS-Port radius

  attributes may not be represented correctly.

  Workaround: Physically move (if possible) the interfaces into ports which can be correctly

  encoded with 4/1/3 bit distribution.

- CSCte48047

  On a ASR 1000 Router Series the output from the **sh platform software status control- processor** may incorrectly indicate that the ESP committed memory is greater than 100%. There is no functional impact due to this.

  Workaround: There are no known workarounds.

- CSCte50863

  An fman_fp core is generated when the Template ACL feature is disabled or enabled several times with 4k PPP sessions with per-user ACLs.

  This condition has been observed, when bringing up 4000 PPP Sessions terminated on PTA with per-user ACLs. With the template ACL feature enabled, only a few templates are created. Disable the template ACL feature and since there are only 4000 PPP Sessions, TCAM exhaustion by this action is not expected. Enable the template ACL feature again. Repeat until an fman_fp core is generated (usually seen within 10 iterations).

  Workaround: Is to tear down PPP Sessions before disabling and enabling the Template ACL feature.

- CSCte55019

  The Cisco ASR 1000 Router crashes when the local-address is configured as '0.0.0.0' under crypto keyring <name>.

  This issue has been seen, when the ASR 1000 Router is loaded with asr1000rp1-adventerprisek9-mz.122-33.1.5.XNF

  Workaround: Is to configure the local-address with a valid ip address.

- CSCte55632

  On a Cisco ASR 1000 Router Series configured with the WCCPv2 feature and processing WAAS traffic (HHTP/FTP), a switchover from the active ESP to the standby ESP may under certain conditions cause the ESP to reset unexpectedly.

  Workaround: There are no known workarounds.

- CSCte57932

  About 10% of the calls will fail with one way audio on the ASR 1000 Router Series.

  This instance may occur, when SIP Endpoints behind a NAT who are called from a H323 trunk and about 10% of the calls will fail with one way audio.

  Workaround: There is no known workaround.

- 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: None

- CSCte62029

  SBC is disabled (via CLI: **no activate**) service does not completely de-activate even though adjacencies, etc. appear to be in down with detached state. Though SBC will re-activate upon executing the **activate** CLI.

  This condition can occur upon de-activation if the following exist:

  1. billing is **enabled**
  2. a Cisco ASR 1000 Router has redundant RP configuration (software or hardware)
  3. SBC incoming SIP call-rate of 20 CPS.

  Workaround: The following steps can be executed as a workaround once in failed state:

  1. **disable** billing via **billing->no activate** CLI
  2. **execute no activate** CLI again for SBC application
  3. re-activate SBC service via **activate** CLI
  4. re-enable billing via **billing->activate.**

- CSCte64156

  Under certain circumstances, the ROMMON variables may show "PLATFORM_MAX_INTERFACES =128K" while there is no "platform max-interface 128k" configured.

  This usually occurs after router reload.

  Workaround: Is to configure "platform max-interface 128k" and then "no platform max-interface 128k". A reboot is recommended afterwards.

- CSCte66782

  VLAN node may become disabled resulting in possible higher latency for priority packets on the ASR 1000 Router Series.

This condition may occur, when configuring model F broadband configuration using ANCP to change the shape rates on individual VLANs, priority propagation at the VLAN node may become disabled resulting in possible higher latency for priority packets.

Workaround: Do not use ANCP to change the VLAN parent shape rate.

- CSCte71456

  Self ping packets are sent by the a Cisco ASR 1000 Router on the serial interfaces and are not applied with Egress feature such as firewall has been used.

  This has been observed, when packets are sent to a self IP Address and are not applied with the Egress features at CPP for serial interfaces. All other packets should be fine in this same environment.

  Workaround: There is no known workaround.

- CSCte74829

  On the Cisco ASR 1000 Router, dsx3LineStatusChange Trap has been seen for index 0. This condition has been observed on SPA OIR, or when creating a ds3 interface on the 1xchOC12-POS SPA.

  Workaround: None

- 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.

- CSCte81385

  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, 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.

- 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.

- 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: None

- CSCte97907

  On a Cisco ASR 1000 Router with 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: None

Release 2.5 Caveats

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

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

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

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

This section consists of the following subsections:

Open Caveats—Cisco IOS XE Release 2.5.2

This section documents possible unexpected behavior by Cisco IOS XE Release 2.5.2

- CSCsu59515

  Telnet inside host from outside the host fails when port 23 is statically allocated on a Cisco ASR 1000 Router.

  Workaround: None

- 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:

  BGP is configured

  More than one equally-good route is available

  BGP is configured to use less than the maximum available number of multipaths

  Workaround: There is no workaround.

  Further problem description: The selection of non-oldest paths as multipaths is only problematic in releases which include CSCsk55120, because in such releases it causes unnecessary changes in whether paths are considered multipaths.

- CSCsz36180

  When **enabling passive header compression** on interface where active header compression is enabled doesn't get reflected in show running configuration of interface. Though its get updated in **show frame-relay map** command output. Also, the header compression is not working as desired after this configuration. Ideally if both side are configured for Passive, compression should not happen. In this case compression is happening though **sh frame relay map** command shows both interfaces are configured as passive on the ASR 1000 Router Series.

  This has been seen, when the following command is used:

```
frame-relay map ip <ip> <dlci> compress passive
frame-relay map ip <ip> <dlci> compress active
```

When the same ip and dlci values are used on the ASR 1000 Router this does not take effect.

Workaround: To do **no frame-relay map ip <ip>** before changing the header-compression from active to passive.

- CSCsz53438

  When ip header compression is configured on the ASR 1000 Router, but not on the corresponding router, an unexpected reload of the embedded systems processor may occur.

  This has been seen, when IPHC is configured on the ASR 1000 Router, but not on the router to which it is directly connected.

  Workaround: Is to **enable IPHC** on both routers.

- CSCta26678

  Unable to add vrf configuration after removal of the same vrf on the ASR 1000 Router Series.

  This has been seen, when ODR is present on the Cisco ASR 1000 Router.

  The router should function normally after the router has been reloaded.

  There are no known workarounds.

- CSCta60589

  On the ASR 1000 Router, when there are files in the tracelog directory doing a wildcard search could potentially result in a CPUHOG message.

  This has been seen, when there are a large number of files in the directory the wild card is being applied on the ASR 1000 Router.

  Workaround: Is to avoid doing wildcards on directories with large number of files.

- CSCtb07144

  Shutting an interface having a large number of vlans while there is a significant number of multicast entries and interfaces in the MFIB database can take a significant amount of time on the ASR 1000 Router Series.

  This has been seen when there are a large number of vlans configured on the interface that is being shutdown. A significant number of entries and interfaces present in the MFIB database.

  Workaround: None

- CSCtb24959

  The ASR 1000 Router Series may fail while clearing large number of rp mappings. This instance can happen when the following has occurred:

  - the router has been configured for rp agent
  - and candidate there are a large number of rp's
  - initiating the **clear ip pim rp-map** command

  Workaround: Is not to apply the **clear ip pim rp-map** command one after the other.

- 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.

- CSCtb40529

  At switchover, the old active takes 2 reboots to become standby for the ASR 1000 Router Series.

  This may occur, when scaled setup with switchover has been configured on the ASR 1000 Router.

  Workaround: None

- CSCtb66050

  On the ASR 1000 Router Series running Session Border Controller (SBC), a traceback is observed on doing an ISSU sub-package upgrade from release 2.5 image to a later image. This traceback is thought to be largely benign and doesn't affect normal operation. Upgrade is successful, calls can be made and media can be set up through SBC.

  This traceback is only observed upon ISSU upgrade from release 2.5 image and only with a sub-package upgrade. The traceback is not seen on performing a consolidated update.

  Workaround: Use a consolidated update procedure instead of sub-package upgrade, when possible.

- CSCtb71415

  There are occasional CPPOSLIB-3-ERROR_NOTIFY: F1 logs from the ASR 1000 standby FP20. The **show plat soft firewall f1 stati** output displays zone-binding ASR 1000 errors may be seen on the ASR 1000 Router console (but not on the active F0). This may occur, when running longevity stress tests incorporating per-subscriber firewall, with redundant RP2 and Topology:

```
stateful PPPoE---LAC--10GbE---LNS---L4-7servers
vanilla PPPoE------|                       |---10GE --tgen

There are 32000 total sessions:
- 12000 are stateful and flapping periodically
- 15000 are vanilla across 3GE ports passing random traffic up 1500B packets at
1.6Gbps upstream total, 2.8Gbps downstream total
- 2500 PSFW sessions just periodically flapping
- 2500 vanilla PPPoE session periodically flapping

Zones are being downloaded via RADIUS.  VFR, uRPF on V-T and/or via RADIUS.
```

  Workaround: No workaround available at this time. In additon the error actually happens during zone unbinding.

- 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 !000 Router.

  Workaround: None

- CSCtb79850

  Interface flap may close when pending channels for the atm spa are configured on the ASR 1000 Router Series.

  This may occur, when the interface flap has pending channels on the atm spa.

  Workaround: None

- CSCtb85661

  On doing multiple switchovers or after ISSU completion followed by a failover, the hardware programming of bidirectional entries doesn't show the correct dest_index (0xFFFF) leading to drop in traffic on the ASR 1000 Router Series.

  Workaround: The dest_index can be set to the correct value using a test cli and traffic resumes.

- CSCtb98877

  On the ASR 1000 Router Series subsequent call fails after a SIP Session Refresh timeout occurs after an HA switchover in CUBE enviroment.

  This occurs in a back to back CUBE environment:

  ```
  CUCM1 - SIP - CUBE1 - SIP - CUBE2 - SIP - CUCM2
  ```

  The CUCM SIP Refresh is set to 90 seconds, and a call is made. HA switchover occurs on CUBE1, and the call is disconnected as expected. The same call is made again, but the originating endpoint on CUCM1 gets a Busy tone, while the terminating endpoint on CUCM2 gets Ringing tone.

  ```
  CUBE2 sends a 503 Internal error with the following cause code:
  Reason: Q.850;cause=38 - [Network out of order]
  ```

  Workaround: None

- CSCtc17366

  Only 1-way media or no media is passng when call setup is establish on the ASR 1000 Router Series. This may occur when SIP trunk has been configurated or any setup using 2 IP adress pair with sport and dport equals 5060 for multiple dialogs on the router.

  Workaround: There is no straight forward workaround other than to put the call on hold, then resume the call to try and recover the media.

- 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.

  When using the following scripts this condition has been seen:

  1. Configuring large mVRF's 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: None

- 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 onbaord disable

  ```
  Router#hw-module slot r0 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.

- CSCtc41808

  When trying to change ipsec tunnel configuration by changing tunnel mode between SVTI and GRE, iosd crash is observed on the ASR 1000 Router Series.

  Workaround: None

- CSCtc50830

  When reloading an active RP just before it goes to rommon mode the ASR 1000 Router dumps a core and crash file pointing to Redundancy FSM.

  This condition happens after IPNAT client reloads the standby RP and synchronizing active with standby.

  Workaround: None

- CSCtc55049

  The ASR 1000 Router may crash 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: None. However if problem manifests, the subsequent rebooting is very likely to be successful. If stuck in a situation where crashes are repetative, momentarily pull redundant RP until system stabilizes, and re-insert redundant RP.

- 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 ocurrs, when BB sessions over ATM PVCs are configured. With a high number of PVCs configured, and if all PVCs are attemtped 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: None. However if problem manifests, a reload of the ESP is required to bring the system back to its normal state.

- CSCtc99048

  When VLAN-VLAN Pseudowires (PWs) redundancy is configured, when the RP switchover happens on pseudowires (PWs) from primary to backup, and the RP is switched back to primary this may not be allowed for some of the pseudowires (PWs) to forward traffic properly.

  Workaround: Is to do a **clear xconnect all** will re-provision xconnect on all PWs, and after that all pseudowires (PWs) can forward traffic properly.

- CSCtd07250

  Acct-Session-Time is inaccurate or incorrect when configured with Session, Traffic-Class Service and Non-Traffic-Class Service Accounting Records on the a Cisco ASR 1000 Router.

  This condition has been observed when, Acct-Session-Time displayed in session-stop records displays values much higher than the actual lifetime of a session.

  In addition, despite the non-TC service having been associated as a active session, for greater than 3-4 seconds, the Acct-Session-Time, in the stop records of such services is displayed as 0.

  Workaround: There is no known 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: No workaround

- CSCtd26479

  On ASR 1000 Router Series, the FP may crash with the following error message:

  ```
  %IOSXE-6-PLATFORM: F0: cpp_ha: Shutting down CPP MDM while client(s) still connected
  ```
  The FP crashes may happen in some instances, when switchover is pushing COA toward PPPoE and there are 1000 PPPoE ISG sessions on the router.

  Workaround: None

- CSCtd26955

  On the ASR 1000 Router Series ANCP sessions may drop with high event rate.

  This condition may occur, when ANCP is configured on ATM (pvc-in-range), the on-demand (AutoVC) is created and enabled at the interface level (with vc-class) on the ASR 1000 Router.

  Workaround: When all the on-demand (AutoVCs) in range is not created on ATM (pvc-in-range), create and enable create on-demand at vc level.

- CSCtd45066

  On the ASR 1000 Router Series the nasport id format is changed between 2.3.0, 2.4.0, 2.5.0 and 2.6.0 releases.

  This condition has been observed when "nas port format d" ***<format>*** is configured on the router.

  Workaround: There is no known workaround at this time.

- CSCtd62837

  H323 to SIP configuration, when the H323 side supports two DTMF methods, the DTMF interworking may fail on the ASR 1000 Router Series.

  When performing H.323 to SIP call, the H.323 side support for H245 alphanumeric userinput and tel-event, the SIP side may just support tel-event. The H.323 side may send DTMF userinput, and the SBC may drop the userinput.

  The following pd log message may appear on console:

  ```
  ICC has failed to find a mechanism to pass on DTMF tones in this call.  The tones will
  not reach their destination.
  ```
  This may not cause the call to fail.

  Workaround: None

- CSCtd87205

  The Cisco ASR 1000 Router will reload, when flapping up and down VC's after configuring SSO.

  This condition has been observed, when the Cisco ASR 1000 Router reloads after a large amounts of flapping has occurred, and SSO has been forced onto the router. The router may reload.

  Workaround: Is to slow down the amount of flapping when doing SSO on the router..

- CSCte19641

  On the ASR 1000 Router Series, the CCP Driver Lockdown crash may happen.

  The following console message has been observed:

  ```
  %CPPDRV-3-LOCKDOWN: F0: cpp_cp:  CPP10(0) CPP Driver LOCKDOWN due to fatal error.
  ```

  This may occur, when stressing the system and activating ISG services with ocasional High Availability (HA) switchover.

  Workaround: None

- CSCte35998

  Secure Media Call will drop during a call if both party's place the call on hold at the same time (or seconds apart) after about 15-20 seconds.

  This condition may occur on a Cisco ASR 1000 Router, when running 2.5.0 release and CUCM - 7.1.3.32010-1.

  Workaround: None

- CSCte62859

  PPP session churn on an LNS following an RP switchover may leave lingering L2TP sessions on the LNS.

  This condition may occur, when session churn is combined with a too-small l2tp receive window size following an RP switchover, lingering PPP sessions can result.

  Workaround: This condition is exacerbated by a too-small l2pt receive window size. Alter this setting according to the number of sessions typically seen on the the tunnel(s) where this situation is observed. Make sure both ends fo the tunnel have similar settings.

- 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: None

- CSCte96759

  IPv6 route summary is incorrect when IPSEC is configured on the Cisco ASR 1000 Router Series.

  This condition can occur when traffic is sent through 500 v6 tunnels.

  Workaround: Is to remove IPSEC on all the tunnels and reconfigure them. This should bring up all the IPSECv6 routes.

- CSCte98852

When broadband accounting accuracy feature (i.e. ‘subscriber accounting accuracy’ CLI is configured) and service accounting is enabled, a duplicate session accounting start (with unique session ID) message is sent out and 2 entries are created on the AAA server.

This feature is specific to ASR 1000 Router. The issue was observed only when the accounting accuracy feature and service accounting are enabled.

Workaround: There is no workaround as the accounting accuracy may be off as much as 10-second worth of byte-counts if the features is turned off, or when the following is configured on the router:

1. ‘aaa accounting delay-start’and
2. aaa accounting include auth-profile [delegated-ipv6-prefix, framed-ip-address, framed-ipv6-prefix]

- CSCtf01109

  The NAS-IP-Address value in the accounting start changes after RP SSO. Before RP SSO, the NAS-IP-Address contains the IP address of the interface connected to the AAA server. After RP SSO, the new active RP sends out a new accounting start. This time, the NAS-IP-Address contains the loopback0 IP address. When the session disconnects, the accounting stop record contains the correct IP address.

  This issue happens in redundant RP system with PPP susbcribers.

  Workaround: There is no known workaround.

- CSCtf05408

  IP address on a loopback interface is lost on the Cisco ASR 1000 Router Series.

  Workaround: Is to reconfigure the loopback interface.

- CSCtf07776

  The below traceback can be seen in two environments on a Cisco ASR 1000 Router:

  – During UUT reload

  – After shutting the FRR enabled interface

  For example the following traceback will appear on the console:

  %FRR_OCE-3-GENERAL: un-matched frr_cutover_cnt.

  -Traceback= 40DCB368 40DCB220 40DCB444 40DEC968 40D15FE4 40D1BACC 40D13BD4 40D14810

  This condition has been seen on the router with TE and FRR enabled on interface during the reboot and issue.

  Workaround: None

- CSCtf27631

  When processing MS-CHAPv2 an unexpected reload may occur on a Cisco ASR 1000 Router.

  This may occur while the ASR 1000 Router is processing an MS-CHAPv2 response in a PPP environment.

  Workaround: None

- CSCtf41625

  In the PE-CE environment, BGP is running between the PE and CE. From the PE , Advertising two prefixes through vrf static routes. These prefixes are not advertised on the CE side.

  This condition can be seen only with global keyword i.e.. next_hop resolution has been applied within the RIB table.

For an example:

ip route vrf vpn1 34.2.0.0 255.255.255.0 Ethernet3/0 34.2.0.2 global

Workaround: There is no known workaround.

- CSCtf44686

  While running in uSBC mode the ASR 1000 Router may crash.

  This condition has been observed when ping-enable is configured under an encrypted adjacency.

  Workaround: None

- CSCtf51373

  The FP crashes on a Cisco ASR 1000 Router running 12.2(33)XNE1.

  This condition may occur when running VOIP traffic.

  Workaround: None

- CSCtf57046

  On a Cisco ASR 1000 Router poor H323 call connection success rate has been seen.

  This problem is caused by a timeout when attemting to open TCP sockets for H245.

  TCP sockets previously timeout after 1 second, which can be the case where there is high latency in the network, or the application with endpoint does not respond within 1 second.

  Workaround: None

- CSCtf57073

  When H323 call setup is done correctly, but there is no audio with video is available on the Cisco ASR 1000 Router.

  This condition is caused by excessive H245 message sizes. Message buffers sizes are not suffient.

  Workaround: None

- CSCtf57132

  Poor video quality for H323 downstreams to H323 calls on the Cisco ASR 1000 Router.

  This condition is caused by Bearer Capabilites in the Q931 Seup, always being changed to 64k.

  Endpoints which choose to apply the bandwidth in Bearer Capabilites (not mandated) will then attempt to open both audio and video to not exceed a total bandwidth of 64k causing poor video.

  Workaround: The bearer capabilites rate mutiplier is now being propagated correctly which resolves the bandwidth issues.

- CSCtf57273

  VRF mapping service on ISG may cause IGP to fail on downstream interface.

  Workaround: None

- CSCtf61700

  Memory leak has been seen when Radius is processed on a Cisco ASR 1000 Router.

  This happens only when Radius Server (ACS) send Access-Reject for a service profile download.

  Workaround: Make sure the respective profile is configured in the ACS (Radius server) that is needed for download.

- CSCtf70365

When config ED is used for EEM with some special config like virtual-template commands, it can trigger more than intended.

When certain commands are configured, this can happen.

Workaround: Is to use syslog ED instead.

Resolved Caveats—Cisco IOS XE Release 2.5.2

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.5.2

- CSCsd39262

  A crash may happen when ACL has no match in a prefix list on a Cisco ASR 1000 Router. When a named acl is first referred by "match ip address" command, followed by a "no match ip address prefix" command which refers to the same ACL name, the router either generates an alignement error or crashs.

  Workaround: There is no workaround.

- CSCsq24672

  A call through CUBE may not establish for a Re-Invite-based call flow. The call may drop.

  This symptom is observed if the endpoint to which the CUBE is communicating sends a Re-INVITE for a call before it has received an ACK from the other call leg for the original INVITE. CUBE may not forward this Re-Invite to the other call leg, and the call will disconnect.

  Workaround: There is no workaround.

- CSCsw44668

  Conditional debugs is not complete on the ASR 1000 Router Series. This condition is more likely to happen when debug is enabled on the tunnel, issuing **shut** and then **no shut**.

  Workaround: None

- CSCsx02819

  When NAT traffic is flowing, if the user tries to delete NAT pool, an error message is displayed and NAT pool is not removed since it is in use. But the NAT pool is removed in the Standby. Due to this, NAT does not work after SSO switchover. In this example the following condition have been observed:

  ```
  (config)#no ip nat pool <name> <start-ip> <end-ip> {netmask <netmask> | prefix-length
  <prefix-length>}
  ```

  Workaround: Is to issue the pool configuration command, after the pool gets deleted in the standby RP, prior to SSO switchover.

- 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: None

- CSCsz82950

  A peer RP reloads on a Cisco ASR 1000 Router. When any configurations are done using NMS for DCTM MIB, this symptom occurs when unconfiguring the configuration that is created by DCTM MIB configuration.

  Workaround: There is no workaround.

Further Problem Description: DCTM was not HA supported before. HA is supported now. If configurations are not done by using NMS, there will not be any issues.

- CSCta12530

  The aggregate-fragment stats are not shown on the primary or secondary link when disjoint policies using service-fragment and fragment are applied on Etherchannel member links with sub-interfaces.

  The problem occurs only when using Etherchannel, with service-fragment policies applied on Etherchannel member links and fragment policies applied on Etherchannel sub-interfaces.

  With this configuration, in the output of **show policy-map interface <*member-link*>** we can see that the aggregate-fragment counters may be missing from one of the member links.

  Workaround: There is no known workaround.

- 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: None

- CSCtb33439

  Hub or spoke crashes when the spoke tunnel is **shut** or **unshut** on a Cisco ASR 1000 Router**.**

  This conditon may occur when applying dmvpn configs after performing a **shut** and **no shut** on the tunnel.

  Workaround: None

- CSCtb66770

  Serial interface are not added as member links to the MLP bundle.

  This condition may occur, after properly configuring a MLP bundle and its member links, flapping of the all the member link interfaces can cause links to not be re-added to the MLP bundle.

  Workaround: None

- CSCtb87546

  Tftp server may times out sometimes or always on the ASR 1000 Router Series. This may occur when uploading or downloading files, including IOS images to tftp server.

  Workaround: Is to use 2.5 pre-released images on the router in order to run the tftp operation successfully.

- CSCtb89424

  In rare instances, a Cisco ASR 1000 Router may crash while using IP SLA UDP Probes configured using SNMP and display an error message similar to the following:

  hh:mm:ss Date: Address Error (load or instruction fetch) exception, CPU

  signal 10, PC = 0x424ECCE4

  This symptom is observed while using IP SLA on the router.

  Workaround: There is no workaround.

- CSCtc18656

  When the NAT box is configured as the Rendezvous Point (RP). This does not allow for source address translation for the encap packet received from the First Hop Router.

  NAT box is configured as Rendezvous Point (RP) decapsulates the packet and forwards it to NAT outside without translation which will create incorrect S,G state for a inside local source address on the downstream routers after NAT router.

  Workaround: None

- CSCtc21042

  A chassis-manager processed on RP2 gets stuck and the router becomes unresponsive to user commands. All the FPs and CCs keep rebooting, with console logs showing repeated FP code downloads. This problem is specific to RP2. No particular scenario is known. Problem is caused by OBFL logging of messages on RP2.

  Workaround: Is to disable onboard logging of messages on RPs as follows:

  "hw-module slot r0/r1 logging onbaord disable"

```
Router#hw-module slot r0 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.

- CSCtc48125

  Duplicated ARP entry when enabling ISG. When you enable ISG for the existing DHCP users, you may see the following:

```
GPKC10ki01#sh arp | i aaaa.bbbb.cccc
Internet  x.x.x.x          -   aaaa.bbbb.cccc  ARPA   GigabitEthernet1/0/2.1203
Internet  y.y.y.y         16   aaaa.bbbb.cccc  ARPA   GigabitEthernet1/0/2.1203
GPKC10ki01#
```

  (The one without the age is the ISG user and the one with an age is the DHCP learned address.)

  The symptom is observed on a Cisco ASR 1000 Router when enabling ISG on existing DHCP users.

  Workaround: Is to disable multiple DHCP servers. Use one DHCP server.

- CSCtc50985

  Output of the **show ip subscriber dangling <*500*>** at a steady state shows lots of sessions of the form:

  dhcp 0000.6401.2a64 [37649] control waiting

  The symptom is observed in large scale scenarios or when CPS is much higher than recommended.

  Workaround: Is to clear the session on the router and reboot, if required.

  Further Problem Description: In scale scenarios, the DHCP handshakes between the client, so the DHCP relay and server might take a long time. Also, the wire or DHCP server is loaded so that it drops some offers or ACKs. In this case, some sessions might be seen dangling without corresponding binding and there is no connectivity to the user.

- CSCtc72651

  A crash has been seen on a new RP after SSO with AToM debugs are enabled on the ASR 1000 Router Series. When enabling AToM debugs which requests VC Accouting details from MFI during SSO the router may fail.

  Workaround: None

- CSCtc78200

  A Cisco ASR 1000 Router may crash in parse_configure_idb_extd_args routine.

  This symptom is observed when running PPP sessions or when TCL is used for configuring interface range.

  Workaround: As the PPP session is being established on the LNS, Cisco IOS will momentarily use one of the available VTYs from the router. After initial configuration, it is immediately released to the system pool.

  When all VTY connections are in use, an RP crash will occur if a new PPP session is established and there are no free VTYs in the system.

  To work around this issue, reserve several VTY connections for PPP session establishment. Since it is possible that a burst of PPP sessions tries to connect using multiple VTY connections at the same time, reserve at least 5 VTY connections. One possible solution is to use an ACL on the last 5 VTY

  lines:

```
ip access-list extended VTY_ACL
 deny   ip any any
!
line vty 5 9
 access-class VTY_ACL in
 exec-timeout 1 0
 login authentication local1
```

  Alternate Workaround: Do not configure “interface range” cli using ios_configfrom tclsh mode. When in tclsh mode, use normal “interface cli” in a “for loop”.

- CSCtc91560

  High CPU utilization occurs on a Cisco ASR 1000 Router.

  The symptom is observed with session churn on the router.

  Workaround: There is no workaround.

  Further Problem Description: CPU usage will remain high under normal conditions given a constant churn rate of approx 24 CPS, coming up and down.

- CSCtc95709

  During ISSU upgrade, the standby router may crash and reload after displaying the following error message:

  DATACORRUPTION-1-DATAINCONSISTENCY or DATACORRUPTION DATAINCONSISTENCY

  This symptom is observed during ISSU upgrade if RPs are in slots between LCs. If RPs are in slots below all LCs, or slots above all LCs, the symptom should not occur.

  Workaround: Physically move RPs to the lowest slot numbers, below the LC slot numbers. Moving RPs one by one should allow continued serviceability.

- CSCtd00493

  For IPv6 Bi-directional entry FF03::1:0:0/96, some packet with address like FF03::1:1:1/128 or FF03::1:1:2/128, etc… In addition a Cisco ASR 1000 Router cannot find a match in CPP due to the collision lookup failure. This problem may cause the traffic to not forward the entries on the router.

  Workaround: None

- CSCtd02123

  WRED state only shows WRED state with standard class.

  In **sh policy-map int**, WRED state only show standard class's WRED state.

  Workaround: Is to only use standard wred classes.

- CSCtd22064

  The ASR 1000 Router Series will crash when removing SBC configuration after a failover.

  During normal call operations a failover is initiated via CLI. Normal call operations continue without issue after the failover. After stopping all calls, the SBC configuration is removed and the Cisco ASR 1000 Router will crash.

  Workaround: Do not remove SBC configuration.

- CSCtd24065

  The output of the command **show subscriber statistics** shows that number of "SHDBs in use" is greater than the total number of unique subscribers for the deployment. This might contribute to issues such as an "out of IDs" message or sessions not coming up.

  The symptom occurs for DHCP-initiated sessions either when:

  1. Session idle times out followed by a lease expiry or you release the lease.
  2. Session is cleared using the **clear subscriber session** command and there is a lease expiry or you release the lease.

  Workaround: There is no workaround.

  Further Problem Description: This can also contribute to a small amount of observed memory leak.

  This problem occurs in code branches where IP session HA is not supported. In these branches, the above steps cause a SHDB handle to not be cleared properly when other datastructures are cleared.

- CSCtd25688

  The Cisco ASR 1000 Router crashed multiple times when using 2.6 pre-released images with the following message:

  Kernel panic - not syncing: Attempted to kill init.

  In some instances this problem may occur with no traffic ON.

  Workaround: None

- CSCtd31226

  Every 10 seconds an error message has been logged on a Cisco ASR 1000 Router console:

  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp: cpp_cp encountered an error

  This error has been seen when using 12.2(33)XND1 release.

  Workaround: There is no known 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.

- CSCtd34644

  Hub and spoke on the ASR 1000 Router Series in DMVPN - Hub Support by QoS Class (DMVPN Phase 3) the network shows ATTN SYNC timeout and IPSEC-3-CHUNK_DESTROY_FAIL messages in steady state traffic and during dmvpn config cleanup. This is seen during scale config and configuration cleanup.

  Workaround: No Workaround

- CSCtd38225

  When ISG is enabled and DHCP sessions re-start just around the time their leases expire, some sessions may get stuck dangling indefinitely. Sending DHCPDISCOVER message (i.e.: re-starting the CPE) will not restore the session. The affected subscriber(s) will not be able to establish a session.

  This condition has been observed whenISG is enabled and DHCP sessions re-start just around the time their leases expire.

  Workaround: The only known workaround is to manually clear the dangling session(s) using the **clear ip subscriber dangling** *<time>* command although this may not be a suitable workaround in a live production network.

- CSCtd39778

  The Cisco ASR 1000 Router may reset due to IOS failure when ZBFW is configured with more than 16 match protocols and there are large an additional no match protocl statements in ZBFW class-maps.

  This has been seen, when an addition of more than 16 match protocol statements in a class-map is used for inspect policymap on the ASR 1000Router.

  Workaround: Is to split the class-map with more than 16 match protocol into multiple class-maps, each with 16 or less match statements.

- CSCtd42810

  PPPoEoA sessions are not coming up because some VCs are in inactive state on the Cisco ASR 1000 Router Series.

  This symptom has been observed when around 400 PVCs are configured with PPPoEoA sessions.

  Workaround: Is to save the configuration on the LAC, then reload the LAC.

- CSCtd42928

  An IP DHCP ISG subscriber session is not being created for a particular subscriber on the Cisco ASR 1000 Router Series. While other subscribers are not affected.

  The symptom is observed under the following conditions:

  1. Scaled environment (with 20k sessions).
  2. Using debugs and show commands it is determined that no session or binding exists for the subscriber, but a DPM context exists.

  Workaround: There is no workaround.

  Further Problem Description: In such conditions the only way to start the session for the subscriber is a reload or switchover.

- CSCtd53112

  IOS reload occurs when on a Cisco ASR 1000 Router when ‘debug cond ip nat inside source static..’ command entered and NAT has never been configured on the box.

  Workaround: Enter 'debug cond ip nat' commands only after NAT has been configured.

- CSCtd60249

  Policy-map counters are not updated randomly on a Cisco ASR 1000 Router running 12.2(33)XND2.

  This condition maybe seen only when when time-based ACL is used for classification.

  Workaround: Is to reconfigure the policy-map.

- CSCtd66132

  On a Cisco ASR 1000 Router FP reloads when changing the RP address with DMVPN Config.

  This problem maybe seen on the ASR1000 Router, when changing the RP address with DMVPN Config, while sending multicast packet.

  Workaround: None

- CSCtd70582

  Traffic Class services will remain in “show subscriber session” output under "Policy Information" after traffic class has disconnected by timer events.

  Only seen when Traffic Class is disconnected through an Idle Timer or Absolute Timer expiring.

  Workaround: When traffic class service is disconnected through normal (User Intervention), issue is not seen. For Timer disconnected Traffic Class services, no known workaround at this time.

- CSCtd72215

  Using 12.2(33)XNE CCO image the following behavior is noticed with an IPv6 enabled interface. Basically, toggling “ipv6 unreachable” config on an interface leads to unreachables being permanently disabled :

  1. Confirm that by default interface responds with ICMPv6 unreachable message when traffic with unknown destination is sent.
  2. Configure “no ipv6 unreachables” on interface and it is observed that ICMPv6 unreachables are no longer sent.
  3. Configure “ipv6 unreachables” on interface ... expect to see unreachables being generated again however this is not the case.

  This condition may happen after configuring “no ipv6 unreachables” and the inablity to configure back to ipv6 unreachables.

Workaround: Is to reload IOS Software.

- CSCtd73567

  The ASR 1000 Series Router may reload unexpectedly while reassembling a fragmented ip packet.

  Workaround: None

- CSCtd75461

  When the same destination ip address is used in multiple netflow exports, of the following syntax, **ip flow export destination**<*ip-address*><*port*>, only the first configured export port will be used to send 1 copy of the export packets. If different destination ip addressses are used, this problem is not seen.

  Additionally, if a destination ip address is configured with an unintended port number, and the user then configures the same statement with the intended port number, both flow exports will show up in the config and in the output of <CmdBold>show ip flow export<noCmdBold>, and if you then delete the first entry, we will still continue to send exports to the originally configured port number for that ip address.

  Workaround: If you can configure two ip addresses on that same destination host, and use separate export statements for sending those packets, then this could be a feasible workaround.

- CSCtd77312

  L2TP resync will fail under some conditions on the ASR 1000 Router Series.

  This condition has been see before RP swichover occurs, when LAC has sent some L2TP control packets which have not been acknowledged yet.

  Workaround: There is no known workaround.

- CSCtd80007

  The standby routing processor crashes during an SSO when TE Auto-Tunnel Backup is enabled on a Cisco ASR 1000 Router.

  The symptom has been observed during an SSO only on a new Standby RP when TE Auto-Tunnel Backup is in use.

  Workaround: Is to disable TE Auto-Tunnel backup.

- CSCtd83822

  Increasing memory usage of ‘reflector.sh’ and ‘droputil.sh’ process may occur on the ASR 1000 Router Series.

  Workaround: None

- CSCtd84427

  After RP2 Switchover, some of the adjacency do not come up on the Cisco ASR 1000 Router Series.

  This condition has been seen when manual switchover on the RP2 has occurred.

  Workaround: None

- CSCtd90979

  When configuring hierachical QoS policy-map with precent based rate configuration, the rate calcultion might be wrong when the QoS policy is applied to 10 GigabitEthernet interface.

  The translation from percent to absolute value (in Kbps) might be wrong when QoS policy is applied to 10 GigabitEthernet interface.

Workaround: To change from using the percent rate to the absolute rate in BPS (bits per second0 in parent shaper would avoid running into this issue.

- CSCte02973

  Routing protocols like EIGRP may be dropped in the global table.

  The symptom is observed when multicast is configured for a VRF and no multicast is configured for the global table.

  Workaround: Is to **enable ip multicast routing** and create a loopback interface with **ip pim sparse-mode enabled**.

  Further Problem Description: The problem should not occur for MVPN since this is not a valid configuration, as multicast in the core is a requirement. However, it can occur for a feature called MVPN-lite, where multicast traffic is routed between VRF tables without the tunneling and therefore without the requirement for multicast in the global table.

- CSCte05357

  The ASR 1000 Router may crash, when bringing up PPPoE sessions after segmentation faults are configured. This has been seen, when bringing up PPPoE with AAA authorization on VRF and PPP configuration with virtual templates is configured on the router.

  Workaround: None

- CSCte05638

  Cannot copy WebEx application logs from WebEx Node SPA console with Vegas shell commands.

  When connection to WebEx Data Center fails, the WebEx support team might need to look at the WebEx application log files to identify the problem.

  There is no mechanism today for customer to copy this logs files out of the WebEx Node SPA.

  Workaround: None

- CSCte07457

  The ASR 1000 Router is showing only zero counters for qos service-policies (as per the show policy-map interface) when applied on Ethernet based interfaces (FE and GigE) after a reload.

  Workaround: None

- CSCte08145

  CPP reset on sending malformed GRQ on the Cisco ASR 1000 Router.

  This condition has been seen after malformed GRQ has passes through the ASR 1000 Router, where router is performing ALG. The CPP will reset after some time period.

  Workaround: There is no workaround as of now.

- CSCte19782

  When ESP traffic is traversing NAT with inside static configs, the traffic initiated from the outside hosts willl not work.

  This condition happens with NAT inside static configuration, the ESP traffic iniitated from the outside network will be passing through the NAT box untranslated.

  Workaround: There is no known workaround.

- CSCte20245

  ESP is observed to reload while trying to bringup PPPoEoA sessions during an RP Switchover.

  This condition has been observed, when PPPoEoA sessions are setup during RP switchover this may cause ESPs to reload.

Workaround: Setup sessions after RP switchover has happened.

- CSCte20928

  ESP20 restarts when loading the config on the RP2.

  This issue has been seen when loading config on a blank box with ESP20 and RP2.

  Workaround: None

- CSCte29294

  On the Cisco ASR 1000 Router the ESP may crash, when doing High Availibility (HA) switchover in LNS environment.

  This has been seen, when LNS has been configured with traffic.

  Workaround: There is no workaround.

- CSCte40621

  On a Cisco ASR 1000 Router when adding pinhole, after modify has failed with an ER=421 error message.

  For example: “AddIssue-NG.pcap” contains failed pattern with following order:

  - ADD (pinhole/user1a)
  - ADD (pinhole/user2a)
  - Modify (pinhole/user1a)
  - ADD (poinhole/ser2v) -> failed with ER=421

  Workaround: None

- CSCte43708

  On a Cisco ASR 1000 Router a crash can occur when using QFP.

  This instance may occur when QFP is forwarding an IP fragment while doing ip virtual-reassembly, which is **enabled** by NAT.

  Workaround: None

- CSCte45106

  Crash in QoS cpp_cp process when memory is running to slow on the Cisco ASR 1000 Router Series . The following conditions have been observed:

  1. Establish 25k PPPoE PTA ISG sessions with traffic classes, port bundle, l4r, accounting and QoS.
  2. Send traffic through the sessions.
  3. Make sure that all the idbs are used.
  4. Keep trying to establish PPPoE sessions.
  5. FP crash should be observed.

  Workaround: Keep memory from running low.

- CSCte45509

  The ASR 1000 Router cannot take over PPP and L2TP sessions when ISSU has been loaded .

  During ISSU step, Active RP image is a previous version and Standby RP image is 12.2(33)XND3.

  The following traceback occurred and cannot create ppp sessions on Standby RP:

  %SYS-2-LINKED: Bad enqueue of xxx in queue xxx -Process= “RADIUS”

Therefore all PPP sessions is lost at the time of RP switchover.

Workaround: There is no workaround.

- CSCte46020

  When using a nas-port-format which is different from default encoding 4/1/3, the NAS-Port-ID and NAS-Port radius attributes do not reflect the requested encoding. This is for sessions which originate on ATM interfaces only, i.e. PPPoEoA.

  Depending on physical interface location, the NAS-Port-ID and NAS-Port radius attributes may not be represented correctly.

  Workaround: Physically move (if possible) the interfaces into ports which can be correctly encoded with 4/1/3 bit distribution.

- CSCte46218

  Traffic is not forwarded through GRE or multipoint GRE tunnels with “tunnel key 0”. This condition is seen when tunnel key is configured via “no tunnel key” and then reconfigured via “tunnel key 0” on a GRE or mGRE tunnel, traffic will received tunnel packets will be dropped.

  Workaround: After removing tunnel key configuration, configure “tunnel key” with non-zero value or delete and recreate tunnel interface.

- CSCte50523

  The H.323 Fast-Slow interworking feature was added in an earlier release of DC SBC, however, the feature is being deprecated.

  This affects the following cli:

  #config t

  Enter configuration commands, one per line. End with CNTL/Z.

  (config)#sbc <name>

  (config-sbc)#sbe

  (config-sbc-sbe)#adj h323 ADJA

  (config-sbc-sbe-adj-h323)#start ?

  fast H.323 Fast start for outgoing calls on this adjacency

  slow is no longer an option meaning Fast Start requests on this adjacency will not be converted to Slow Start.

  Workaround: This is a deprecation of a cli and no work around is needed.

- CSCte50685

  NAT DNS ALG TTL not set to 0. Failover from primary ASR to secondary will cause application failure because of invalid dns cache entries from old nat. By setting the TTL to 0 the client will rerequest dns information.

  Workaround: None

- CSCte50721

  During stateful NAT sync of H323 information from primary to standby, the standby crashes.

  This condition occurs when Cisco ASR 1000 Router with dual RP and ESP configured.

  Workaround: Is to disable H323 with the following commands when H323 ALG is not required:

  no ip nat service h225

  no ip nat service ras

- CSCte51283

  Traffic on a priority class receives more bandwidth than what has been configured.

  This condition has been observed when configuring “priority percent” on a QOS service-policy, if the class-default has “fair-queue” configured, the rate on the priorit

  Workaround: None

- CSCte51436

  Pressing Hold during a SIP-to-SIP call through CUBE(Ent) on the ASR 1000 Router results in intermittent disconnects. The phone behind the ASR CUBE hears a fast busy tone.

  When CUBE dial-peers are configured with dtmf-relay of: “rtp-nte”, “sip-notify rtp-nte”, or none.

  ASR CUBE(Ent) version from CCO: asr1000rp2-adventerprisek9.02.05.00.122-33.XNE.bin

  Workaround: Is to use “sip-notify” as the dtmf-relay method.

- CSCte52369

  On a Cisco ASR 1000 router, the RADIUS will send a NACK for the First COA request message and Radius Authentication will fail.

  This condition has been observed when the RADIUS recieves “ACCESS-ACCEPT” with ‘Unsupported Vendor’ attribute.

  Workaround: Is to send the COA request message again.

- CSCte56627

  Outside NAT sessions are not syncing between active and standby.

  The following symptom may occur:

  1. Sessions may not be sync properly to standby OR
  2. ession deletes may not be sync properly to standby (session that would be deleted on standby, will not be deleted).

  The following conditons may occur:

  1. On ASRNAT when there is an inside mapping and outside static mapping configuration.
  2. When there is a very high burst of session aging occurs.

  Workaround: None

- CSCte58825

  There is a crash upon conducting an snmpwalk from “enterprise mib oid 1.3.6.1.4.1”.

  The symptom is observed on a Cisco ASR 1000 Series Aggregation Services router that is running Cisco IOS Release 12.2(33)XNE.

  Workaround: Configure SNMP view to exclude ipsecpolmap as follows:

  snmp-server view <view name> iso included

  snmp-server view <view name> ipsecpolmaptable excluded

- CSCte60069

  During the scale testing with ModelF applied on PTA, reparenting operation results in FP crash. Also CPUHOG and TIMEHOG tracebacks observed. The following conditions have been seen:

  1. On PTA, bring up 24K IPv4 sessions, 2PQ+2CQ (modelf)
  2. remove grandparent shaper and3)add the shaper back. When this instance occurs, FP crashes a tracebacks are observed.

Workaround: Without the fix for this ddts, avoiding reparenting with large number of vlans with sessions will resolve the issue.

Open Caveats—Cisco IOS XE Release 2.5.1

This section documents possible unexpected behavior by Cisco IOS XE Release 2.5.1

- CSCsz36180

  When **enabling passive header compression** on interface where active header compression is enabled doesn't get reflected in show running configuration of interface. Though its get updated in **show frame-relay map** command output. Also, the header compression is not working as desired after this configuration. Ideally if both side are configured for Passive, compression should not happen. In this case compression is happening though **sh frame relay map** command shows both interfaces are configured as passive on the ASR 1000 Router Series.

  This has been seen, when the following command is used:

  ```
  frame-relay map ip <ip> <dlci> compress passive
  frame-relay map ip <ip> <dlci> compress active
  ```
  When the same ip and dlci values are used on the ASR 1000 Router this does not take effect.

  Workaround: To do **no frame-relay map ip <ip>** before changing the header-compression from active to passive.

- CSCsz53438

  When ip header compression is configured on the ASR 1000 Router, but not on the corresponding router, an unexpected reload of the embedded systems processor may occur.

  This has been seen, when IPHC is configured on the ASR 1000 Router, but not on the router to which it is directly connected.

  Workaround: Is to **enable IPHC** on both routers.

- CSCta26678

  Unable to add vrf configuration after removal of the same vrf on the ASR 1000 Router Series.

  This has been seen, when ODR is present on the Cisco ASR 1000 Router.

  The router should function normally after the router has been reloaded.

  There are no known workarounds.

- CSCta60589

  On the ASR 1000 Router, when there are files in the tracelog directory doing a wildcard search could potentially result in a CPUHOG message.

  This has been seen, when there are a large number of files in the directory the wild card is being applied on the ASR 1000 Router.

  Workaround: Is to avoid doing wildcards on directories with large number of files.

- CSCta65347

  CME is changing the media direction attribute as “INACTIVE” instead of “RECVONLY”on the ASR1000 Router Series.

  Only in this instance the resume fails, when CCM/CME scenario's from h323 legcalls are used and there is no media on the ASR 1000 Router.

  Workaround: None

- CSCtb07144

  Shutting an interface having a large number of vlans while there is a significant number of multicast entries and interfaces in the MFIB database can take a significant amount of time on the ASR 1000 Router Series.

  This has been seen when there are a large number of vlans configured on the interface that is being shutdown. A significant number of entries and interfaces present in the MFIB database.

  Workaround: None

- CSCtb24959

  The ASR 1000 Router Series may fail while clearing large number of rp mappings. This instance can happen when the following has occurred:

  - the router has been configured for rp agent
  - and candidate there are a large number of rp's
  - initiating the **clear ip pim rp-map** command

  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: None

- 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.

- CSCtb40529

  At switchover, the old active takes 2 reboots to become standby for the ASR 1000 Router Series.

  This may occur, when scaled setup with switchover has been configured on the ASR 1000 Router.

  Workaround: None

- CSCtb56852

  RP resets when we delete DMVPN Tunnel on hub router .

  In 1hub and 1000 spokes scenario, when we delete dmvpn tunnel on hub causes RP reset on hub router.

  Workaround: None

- CSCtb66050

  On the ASR 1000 Router Series running Session Border Controller (SBC), a traceback is observed on doing an ISSU sub-package upgrade from release 2.5 image to a later image. This traceback is thought to be largely benign and doesn't affect normal operation. Upgrade is successful, calls can be made and media can be set up through SBC.

  This traceback is only observed upon ISSU upgrade from release 2.5 image and only with a sub-package upgrade. The traceback is not seen on performing a consolidated update.

  Workaround: Use a consolidated update procedure instead of sub-package upgrade, when possible.

- CSCtb71415

  There are occasional CPPOSLIB-3-ERROR_NOTIFY: F1 logs from the ASR 1000 standby FP20. The **show plat soft firewall f1 stati output** displays zone-binding ASR 1000 errors may be seen on the ASR 1000 Router console (but not on the active F0).

  This may occur, when running longevity stress tests incorporating per-subscriber firewall, with redundant RP2 and Topology:

```
stateful PPPoE---LAC--10GbE---LNS---L4-7servers
vanilla PPPoE------|                       |---10GE --tgen

There are 32000 total sessions:
- 12000 are stateful and flapping periodically
- 15000 are vanilla across 3GE ports passing random traffic up 1500B packets at
1.6Gbps upstream total, 2.8Gbps downstream total
- 2500 PSFW sessions just periodically flapping
- 2500 vanilla PPPoE session periodically flapping

Zones are being downloaded via RADIUS.  VFR, uRPF on V-T and/or via RADIUS.
```

  Workaround: No workaround available at this time. In additon the error actually happens during zone unbinding.

- 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 !000 Router.

  Workaround: None

- CSCtb79850

  Interface flap may close when pending channels for the atm spa are configured on the ASR 1000 Router Series.

  This may occur, when the interface flap has pending channels on the atm spa.

  Workaround: None

- CSCtb98877

  On the ASR 1000 Router Series subsequent call fails after a SIP Session Refresh timeout occurs after an HA switchover in CUBE enviroment.

  This occurs in a back to back CUBE environment:

  CUCM1 - SIP - CUBE1 - SIP - CUBE2 - SIP - CUCM2

  The CUCM SIP Refresh is set to 90 seconds, and a call is made. HA switchover occurs on CUBE1, and the call is disconnected as expected.

  The same call is made again, but the originating endpoint on CUCM1 gets a Busy tone, while the

terminating endpoint on CUCM2 gets Ringing tone.

CUBE2 sends a 503 Internal error with the following cause code:

Reason: Q.850;cause=38 - [Network out of order]

Workaround: None

- CSCtc16232

  When the L2 MAC address of an Ethernet interface is changed on the ASR 1000 Router Series, the final RA is not sent to the remote endpoint.

  The expected behaviour is that when the L2 MAC address is changed, on the ASR 1000 Router is to send a final RA to the endpoint indicating the change.

  Workaround: None

- CSCtc17366

  Only 1-way media or no media is passng when call setup is establish on the ASR 1000 Router Series. This may occur when SIP trunk has been configurated or any setup using 2 IP adress pair with sport and dport equals 5060 for multiple dialogs on the router.

  Workaround: There is no straight forward workaround other than to put the call on hold, then resume the call to try and recover the media.

- 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.

  When using the following scripts this condition has been seen:

  1. Configuring large mVRF's 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: None

- CSCtc21042

  When MVPN is configured the cman fp crashes and the ESP20 continues to reboot while crypto traffic runs for several hours without triggering any events on the ASR 1000 Router.

  This has been seen, when crypto traffic passes through the system for several hours before this crash takes place.

  Workaround: None

- CSCtc41808

  When trying to change ipsec tunnel configuration by changing tunnel mode between SVTI and GRE, iosd crash is observed on the ASR 1000 Router Series.

  Workaround: None

- CSCtc50830

  When reloading an active RP just before it goes to rommon mode the ASR 1000 Router dumps a core and crash file pointing to Redundancy FSM.

  This condition happens after IPNAT client reloads the standby RP and synchronizing active with standby.

  Workaround: None

- CSCtc55049

  The ASR 1000 Router may crash 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: None. However if problem manifests, the subsequent rebooting is very likely to be successful. If stuck in a situation where crashes are repetative, momentarily pull redundant RP until system stabilizes, and re-insert redundant RP.

- CSCtc71338

  When configuring a 10k line ACL (production-out) on the interface, the FP process crashes on the ASR 1000 Route Series.

  The production-out will show as follows:

```
interface GigabitEthernet0/3/4
 ip address 1.10.4.1 255.0.0.0
 ip access-group production-out in
 ip access-group production-out out
 speed 100
 no negotiation auto
 cdp enable
 service-policy output test
```

  Workaround: None

- 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 ocurrs, when BB sessions over ATM PVCs are configured. With a high number of PVCs configured, and if all PVCs are attemtped 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: None. However if problem manifests, a reload of the ESP is required to bring the system back to its normal state.

- CSCtc90996

  While under load for extended periods of time, a condition may ocurr that causes a large amount of stale call legs to exhibit on the ASR1000 Router Series. These stale call legs can consume enough memory on the platform to cause a crash due to memory outage. It has been observed with 2000 active calls at 20 CPS for an extended period of time.

  Workaround: To avoid a runaway condition, the use of the command max-conn on the dial-peers of the platform is capable of holding back the amount of stale call legs. While the condition occurs that triggers the event, max-conn has the side effect of not permitting calls to be established over this dial-peer. Eventually it will clear and calls may continue.

- CSCtc95709

  During ISSU upgrade on the ASR 1000 Router Series, there may be two symptoms:

  1. Error message DATACORRUPTION-1-DATAINCONSISTENCY or DATACORRUPTION DATAINCONSISTENCY printed out
  2. Standby may crash and reload

  This problem may occur, during ISSU upgrade, while RP's are configured for slots between LC's. When RP's are in slots below all LC's, or slots above all LC's, the problem should not occur.

  Workaround: Is to physically move RP's to the lowest slot numbers, below the LC's slot numbers. Moving RP's one by one should allow for continued serviceability.

- CSCtc99048

  When VLAN-VLAN Pseudowires (PWs) redundancy is configured, when the RP switchover happens on pseudowires (PWs) from primary to backup, and the RP is switched back to primary this may not be allowed for some of the pseudowires (PWs) to forward traffic properly.

  Workaround: Is to do a **clear xconnect all** will re-provision xconnect on all PWs, and after that all pseudowires (PWs) can forward traffic properly.

- CSCtd11492

  Policy on some of the tunnels may continue to stay in a suspended state for typically 4 to 5 minutes on the ASR 1000 Router Series.

  This may occur when tunnels are configured, after executing **shut/no shut** command on the ASR 1000 Router.

  Workaround: None

- 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: No workaround

- CSCtd24611

  When Standby FP is out of memory on the ASR 1000 Router Series, the cpp_cp tracebacks and **FMFP-3-OBJ_DWNLD_TO_CPP_FAILED** messages may appear on the console.

  This text is similar to the following that is printed on the console, the cpp-cp_Fx-0.log error message:

  ```
  cpp_qos_policer_event:1766:EVENT fail to allocate a feature object 0xc (Cannot
  allocate memory)
  ```

  This instance can happen when the following has occurred:

  1. Bringup the ASR with RLS6 image
  2. Initiate 32k PPPoE sessions and send traffic
  3. Start a script which changes the QoS on the PPPoEoQinQ sessions through CoA
  4. Start a script which flaps 4000 PPPoEoA sessions once in every 20mins. cpp_cp tracebacks and FMFP-3-OBJ_DWNLD_TO_CPP_FAILED messages are seen after sometime.

  Workaround: None

- CSCtd26479

  On ASR 1000 Router Series, the FP may crash with the following error message:

  ```
  %IOSXE-6-PLATFORM: F0: cpp_ha: Shutting down CPP MDM while client(s) still connected
  ```

  The FP crashes may happen in some instances, when switchover is pushing COA toward PPPoE and there are 1000 PPPoE ISG sessions on the router.

  Workaround: None

- CSCtd26955

  On the ASR 1000 Router Series ANCP sessions may drop with high event rate.

  This condition may occur, when ANCP is configured on ATM (pvc-in-range), the on-demand (AutoVC) is created and enabled at the interface level (with vc-class) on the ASR 1000 Router.

  Workaround: When all the on-demand (AutoVCs) in range is not created on ATM (pvc-in-range), create and enable create on-demand at vc level.

- CSCtd31447

  On the ASR 1000 Router Series may crash when reloading the QoS configuration.

  This has been seen when switch over is performed on the ASR 1000 under traffic load.

  Workaround: None

- 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.

- CSCtd39409

  IOSD crash on the ASR 1000-WATCHDOG: Process = L2TP mgmt daemon has been seen on the ASR 1000 Router Series.

  This condition has been seen, when flapping on LNS firewall sessions over time happens on the router.

  Workaround: None

- CSCtd39778

  The Cisco ASR 1000 Router may reset due to IOS failure when ZBFW is configured with more than 16 match protocols and there are large an additional no match protocl statements in ZBFW class-maps.

  This has been seen, when an addition of more than 16 match protocol statements in a class-map is used for inspect policymap on the ASR 1000Router.

  Workaround: Is to split the class-map with more than 16 match protocol into multiple class-maps, each with 16 or less match statements.

- CSCtd47503

  On ASR 1000 Router Series, the FP may reboot itself with the following traceback message:

  ```
  %CPPHA-3-FAULT: F0: cpp_ha:  CPP:0 desc:CPP Client process failed: FMAN-FP det:HA
  class:CLIENT_SW sev:FATAL id:1 cppstate:RUNNING res:UNKNOWN flags:0x0 cdmflags:0x0
  %IOSXE-6-PLATFORM: F0: cpp_ha: Shutting down CPP MDM while client(s) still connected
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp:  cpp_cp encountered an error -Traceback=
  ```

  This may occur under stress conditions, when sending Change of Authorization (COA) pushes to deactivate and activate ISG services after RP switchover.

  Workaround: None

- CSCtd56393

  IPsec polo transactions are not complete and spd map id is missing ASR 1000 Router Series. When reconfigurating DMVPN Phase3 hierarchial topology to a single hub (DMVPN Phase)topology this polo issue has been seen.

  To recover from the state, ASR 1000 Router will need to be reloaded.

  In addition, after multiple spoke extremely high scaling tests [config, removal], and changing from hierarchial topology to single hub topology this same problem has been observed.

  Workaround: None

- CSCtd62837

  H323 to SIP configuration, when the H323 side supports two DTMF methods, the DTMF interworking may fail on the ASR 1000 Router Series.

  When performing H.323 to SIP call, the H.323 side support for H245 alphanumeric userinput and tel-event, the SIP side may just support tel-event. The H.323 side may send DTMF userinput, and the SBC may drop the userinput.

  The following pd log message may appear on console:

  ```
  ICC has failed to find a mechanism to pass on DTMF tones in this call.  The tones will
  not reach their destination.
  ```

  This may not cause the call to fail.

  Workaround: None

- CSCtd73567

  The ASR 1000 Series Router may reload unexpectedly while reassembling a fragmented ip packet.

  Workaround: None

- CSCtd83047

  When scaling ODR to 700 routes are missing in fman rp process on a Cisco ASR 1000 Series Router.

  This may occur when the ASR 1000 router is configuring a large number of ODRs.

  Workaround: Is to configure no more than 700 routes.

- CSCtd89804

  A Cisco ASR 1000 Router will bring up sessions very slow, when l2tp tunnel receive-window is set to 4 on LAC and LNS.

  This may happen, when the receive-window value is low on LAC & LNS.

  When the value is left at 4 on the (UUT) LAC and changed to 100 on the LNS, then the CPS is not slow on the router.

  Workaround: Is to leave the receive-window value to 4, as expected on the LAC (UUT) change the value on the LNS to a higher number such as 100.

- CSCtd90979

  When configuring hierachical QoS policy-map with precent based rate configuration, the rate calculation may be wrong, the QoS policy is applied to 10 GigabitEthernet interface on the ASR 1000 Router Series.

  This has been observed, when the translation from percent to absolute value (in Kbps) might be wrong and the QoS policy is applied to 10 GigabitEthernet interface on the router.

  Workaround: Is to change from using the percent rate to the absolute rate in BPS (bits per second) in parent shaper would avoid running into this issue.

- CSCte05357

  The ASR 1000 Router may crash, when bringing up PPPoE sessions after segmentation faults are configured.

  This has been seen, when bringing up PPPoE with AAA authorization on VRF and PPP configuration with virtual templates is configured on the router.

  Workaround: None

- CSCte14955

  An unexpected reload may happen on the ASR 1000 Router Series.

  This has seen, when BGP VPNv4 is configured and a neighbor is flapping on the router.

  Workaround: None

- CSCte19606

  On the ASR 1000 Router a lot of messages may flood the console.

  The following message is observed on the router console:

  ```
  %INTERFACE_API-3-IFNUMTOIDBERROR: Error occurred while using the ifnum to idb table
  for interface Virtual-Access5562, if number 0, during Element Insertion
  %COMMON_FIB-2-IF_NUMBER_ILLEGAL: Attempt to create CEF interface for
  Virtual-Access5562 with illegal if_number: 0  %IDBINDEX_SYNC-3-IDBINDEX_ASSIGN: Failed
  to assign an index to IDB type 21, for interface "" (rc=11) -Process= "VTEMPLATE
  Background Mgr", ipl= 0, pid= 111
  ```

  This may occur under stress conditions, when sending Change of Authorization (COA) pushes to deactivate and activate ISG services with ocasional RP switchover.

  Workaround: None

- CSCte19641

  On the ASR 1000 Router Series, the CCP Driver Lockdown crash may happen.

  The following console message has been observed:

  ```
  %CPPDRV-3-LOCKDOWN: F0: cpp_cp:  CPP10(0) CPP Driver LOCKDOWN due to fatal error.
  ```

  This may occur, when stressing the system and activating ISG services with ocasional High Availability (HA) switchover.

  Workaround: None

- CSCte33491

  The sessions may fail to established on LNS with per-subscriber firewall when configured with zone membership on the ASR 1000 Router Series.

  This may occur when LNS is configured with virtual templates that contain zone membership and uRPF configurations. RADIUS config includes virtual-framentation re-assembly (VFR) and alternate zone membership. In addition, the subscribers may have the RADIUS-directed changes applied to the virtual access interface on the router.

Workaround: Potential work-around is to remove VFR from RADIUS config, since it is automatically configured with firewall.

- CSCte58825

  The ASR 1000 Series Router running release Version 12.2(33)XNE may crash upon snmpwalk from enterprise mib oid 1.3.6.1.4.1.

  The conditions are that the ASR 1000 Series Router is running release Version 12.2(33)XNE (that is, Cisco IOS XE Release 2.5.0).

  Workaround: Configure the SNMP view to exclude ipSecPolMap as follows:

```
snmp-server view <view name> iso included
snmp-server view <view name> ipSecPolMapTable excluded
snmp-server community <community string> view <view name> RO
```

Resolved Caveats—Cisco IOS XE Release 2.5.1

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.5.1

- CSCin99554

  The ASR 1000 Router may hang, when stopping a core dump in progress by pressing the CTRL SHIFT 6 keys.

  This symptom has been observed, only when RCP is used for a core dump.

  Workaround: Do not use RCP for a core dump.

- CSCsc98813

  When using a route-map to set the metric for redistributed static routes, initially the RIP table looks correct on on the ASR 1000 Router. In addition, after sending the second update this changes the hop count for other routes in the RIP table that have not been redistributed on the router.

  Workaround: Instead of using a route-map, use the metric command on the redistribution line, however this will not allow for any filtering.

- CSCsq42904

  On the ASR 1000 Router Series, when there are 1000 characters on the console, if there are more to display, the display is truncated.

  The problem happens when you have a large number of interfaces and the output of “show zone security” is larger than 1000 characters.

  Workaround: The workaround is to show all interfaces and get the zone membership from the interface.

  Further Problem Description: The root cause of the problem is that the display buffer for this command is limited with 1000 characters.

- CSCsr40074

  On the ASR 1000 Router Series the output of **show ip virtual-reassembly** command does not obey terminal length settings and can continue on.

  This will only happen, when there are alot of virtual access interfaces configured on the router.

  For example, in the following sequence in per-subscriber firewall, when there are hundreds or thousands of virtual access interfaces, the output can render the console useless.

  Workaround: There is no workaround.

- CSCsx10028

  A core dump may fail to write or write very slowly (less than 10KB per second).

  The symptom has been observed, when the cause of the crash has occurred, after the memory corruption has happened on the ASR 1000 Router.

  This may occur, when the memory pool has corrupted and the memory cannot be used to write to the core dump. This issue will most likely cause the router to fail. (IO memory corruption crashes should not have this problem.)

  Workaround: There is no workaround.

  Further Problem Description: When increasing the default size for the exception memory region to 256K to make sure it has enough memory to handle writing core dumps. This means that it is no longer be necessary to adjust the default size for the exception memory region as per the core dump instructions on CCO.

- CSCsx59262

  OSPF Neighbors on the ASR 1000 Router may bounce after changing the config-register.

  This condition may occur, after OSPF interfaces and are configured with fast hellos. In addition, when OSPF neighbors is configurated and the value 'config-register' is changed this may cause the router to bounce.

  Workaround: Is to use Bi-directional Forwarding (BFD).

- CSCsx83443

  Iskmp debug messages from all peers are shown in the term monitor enable tty and vty's

  even though **debug crypto condition peer ipv4 x.x.x.x** is set. This is seen on the ASR 1000 Router Series when using peer ip based debug condition. In addition, when using peer ip based debug condition on the router.

  Workaround: None

  Further Problem Description: Only a subset of the messages are shown.

- CSCsy45371

  The **clear ip nat tr *** command removes corresponding static NAT entries from the running configuration, but removing static NAT running configuration does not remove the corresponding NAT cache.

  This may occur, when NAT commands are entered while router is processing around 1 Mb/s NAT traffic.

  Workaround: Is to stop the network traffic while configuring NAT.

- CSCsz56462

  Configuring **cdp run** does not bring up cdp on the interfaces.

  This may only happens, when the default behaviour of a platform is to have CDP disabled.

  Workaround: Is to configure cdp enable on required interfaces.

- CSCsz59469

  On the ASR 1000 Router Series, when the software version of the Active and Standby RP do not match, the Standby RP can reload indefinitely.

  This may occur, when different versions of software are on the Active and Standby RP.

  Workaround: Is to load compatible versions of software on the Active and Standby RP.

- CSCsz66060

  When saving the half duplex vrf configuration and after rebooting the ASR 1000 Router, the half duplex vrf configuration does not apply to the router, anymore.

  This problem only happens, after half duplex vrf has been configured and when the ASR 1000 Router has been rebooted.

  Workaround: Is to re-enter the half duplex vrf configuration again.

- CSCsz66060

  When saving the half duplex vrf configuration and after rebooting the ASR 1000 Router, the half duplex vrf configuration does not apply to the router, anymore.

  This problem only happens, after half duplex vrf has been configured and when the ASR 1000 Router has been rebooted.

  Workaround: Is to re-enter the half duplex vrf configuration again.

- CSCta73008

  Authenticate-req packets recieved out of phase is getting processed and reply has sent on the ASR 1000 Router Series.

  This may occur, when the PPPoE session is UP after the Authenticate-Req with wrong ID/username has injected, while getting processed by the other end and a reply has been sent. This will cause a bit CPU usage and Non-RFC compliance.

  Workaround: None

- CSCtb13421

  The GM may not register on a Cisco ASR 1000 Router Series.

  This symptom has been observed, when a crypto map with local-address is configured and applied on multiple interfaces, after one of these interfaces are then **shut**.

  Workaround: Is to disable local-address for the crypto map.

- CSCtb18426

  The multicast error messages and tracebacks can sometimes be observed when configuring/unconfiguring multicast on an interface using commands with this format **[no]ip pim** on a Cisco ASR 1000 Router Series.

  Usually most multicast configuration have been removed when leaving the last interface still configured on the router. When unconfiguring multicast on the last interface followed by reconfiguring multicast on an interface may result in the multicast error messages being generated. The problem is most likely to occur, when making the configuration changes to virtual interfaces e.g Loopback and Tunnel.

  Workaround: A workaround would be to introduce a time delay between completely unconfiguring multicast and reconfiguring it.

  Further Problem Description: The problem is a consequence of disabling and quickly re-enabling multicast as a result of interface configuration changes. The multicast processes take a finite time to stop and start and can sometimes experience a condition when clean-up of internal data structures is performed under usual conditions. In this case the error messages are generated and full recovery is achieved. There is no known functional or performance impact.

- CSCtb37492

  PIM assert does not occur on a upstream router on which the source address is NATed.

NATed and a downstream router constantly exchange assert/prune message due to the fact that the “source-field” of assert-msg is not subject to NAT in the NATed router.

This occurs when more than one link exists between the two routers.

Workaround: None

- CSCtb40999

  AutoVC behavior is different in standby after SSO on the ASR 1000 Router Series has been configured.

  This has been seen, when AutoVC is configured in a range, and a pvc-in-range is configured for no autovc. In addition, after doing SSO, the VC is in IN state.

  AutoVC should not be displayed in "show atm vc" if it is configured in range.

  Workaround: None

- CSCtb74547

  The ASR 1000 Router Series DMVPN HUB reloads when processing IPSEC key engine.

  This conditions happens when dual DMVPN with shared tunnel protection feature is enabled.

  Workaround: None

- CSCtb86811

  On the ASR 1000 Router Series the following error message may state:

  `“%MFI_LABEL_BROKER-3-MULTIPLE_BIND”`
  within Standby mode, after initiating the **configure replace** command.

  This may occur, when there are large vrf scalability configurations, after static routes are in use in conjunction with **encapsulation ppp** and **mpls label mode all-vrfs protocol all-afs per-vrf**.

  Workaround: There is no workaround for this specific command sequence and configuration.

- CSCtc03750

  SSO switchover may fail, when secondary reloads continuously happens on the ASR 1000 Router Series.

  This has been seen, when L2VPN and L3VPN with Traffic engineering is configured and SSO has been issued SSO on the router.

- CSCtc12334

  The ASR 1000 Router Series may fail when initiating "clear ip bgp " command.

  This command deletes all bgp neighbor relationships and clears bgp RIB.

  This can occur when the following has been configured:

  1. Need to have MDT configured on the router
  2. Need to issue "clear ip bgp " command

  Workaround: None

  Further Problem Description: **clear ip bgp *** is not a command to be used by any operator in a production network the impact is wide and huge.

- CSCtc21191

  MSDP SA messages are not being forwarding to peers when MSDP is up after traffic starts on a Cisco ASR 1000 Router.

  Workaround: Is to start MSDP before traffic starts on the router.

- CSCtc24325

  On a Cisco ASR 1000 Router the **protocol ppp dialer** is getting nv-gened, when dial-pool number is configured on the interface. This command is currently not there in vc-class mode. As a result of this line by line sync to standby fails and standby resets.

  The problem has been seen, when dial pool number is configured on the router.

  Workaround: None

- CSCtc39018

  On a Cisco ASR 1000 Router the **show hw-module subslot X/Y transceiver Z** command shows incorrect voltage.

  Workaround: No known workaround.

- CSCtc40677

  When the distribute list is applied to the virtual template the distribute-list applied to the virtual-template interface is not effective for the virtual-access interfaces spawned by that template.For example, when the ASR 1000 router (hub) is configured as:

```
router eigrp 1
 redistribute static metric 10000 100 255 1 1500
 network 10.0.0.0
 no auto-summary
 distribute-list prefix TEST out Virtual-Template1!
ip route 0.0.0.0 0.0.0.0 Null0
ip route 10.0.0.0 255.0.0.0 Null0!
ip prefix-list TEST seq 10 permit 0.0.0.0/0
ip prefix-list TEST seq 20 permit 10.0.0.0/8
```

  For example:on the branch site when connected to a Virtual-accessinterface will show as:

```
ranch#sh ip route eigrp
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, *15:56:44.397 BRU Wed Oct 7 2009
10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D       10.0.0.0/8 [90/46251776] via 10.12.0.2, 00:00:06, Dialer1
D       10.1.1.0/24 [90/46228736] via 10.12.0.2, 00:00:06,Dialer1
D       10.2.2.0/24 [90/46354176] via 10.12.0.2, 00:00:06, Dialer1
D*EX 0.0.0.0/0 [170/46251776] via 10.12.0.2, 00:00:06, Dialer1
```

  For example: note that there is no filtering applied.

  In rare conditions this error may have occurred on the ASR 1000 router (hub) running 12.2(33)XND1 or later releases.

  Workaround: Is to configure the distribute-list for the specific virtual-access interface used for the connections on the hub.

- CSCtc43110

  Under H.323 call scenarios, outgoing H.323 signaling packets (TCP) are marked with a non-zero DSCP value, even though no QoS is configured for H.323 calls. This happens under all H.323->H.323 and SIP->H.323 scenarios when SBC creates a downstream H.323 calls.

  Workaround: There is no workaround with SBC configuration. QoS can be re-marked when MQC policy is placed on the outbound physical interfaces of the ASR 1000 Series Router.

  Workaround: None

- CSCtc65431

  VPN routes are not added after deleting and then reconfiguring VRF on a Cisco ASR 1000 Router.

  This may occur, when vrf is deleted and added back onto the router.

Workaround: Is to do **clear ip bgp *** or **clear ip bgp x.x.x.x.**

- CSCtc69100

  PCD shows incorrect 'memory requested' output when activated on a Cisco ASR 1000 Router.

  This may occur, when PCD is configured with the following buffer-size and num-buffer:

```
! base configuration
per-call buffer-size debug 1000
per-call export primary harddisk: secondary harddisk:
per-call trigger sip-message 487
!

asr10-rp2(config)#per-call num-buffer 3000
asr10-rp2(config)#per-call active deb
 70 percent of the largest available memory block on the router =
        2061936265 bytes
 Total PCD memory requested by user = 18446744072414584320 bytes
 Not enough memory available on the router.
asr10-rp2(config)#per-call shut
```

  Workaround: None

- CSCtc69991

  When the Cisco ASR 1000 Router is configured as DMVPN spoke may throw tracebacks.

  This may happen, when ODR is configured as the overlay routing protocol and **shut/no shut** is done on the tunnel interface.

  Workaround: Is to use EIGRP as the overlay routing protocol.

- CSCtc76353

  Multilink fails to come up after SSO/PPP Bad Bind messages have been seen when enabling debug PPP negotiation on the ASR 1000 Router Series.

  This problem has been observed, when MLP is configured between two boxes, and only the PEER is configured for MCMLP.

  Workaround: Is to configure both boxes for MCMLP.

- CSCtc78938

  After configuring 6RU Superpackage for ISSU, when loading an image in 2.5.0 Release to the Router1-RP1 and the image in 2.5.0 Release to the Router2-RP1 for a PE router, some ATMoMPLS Pseudowires fail to download to FMAN-FP and QFP. This configuration may cause all traffic sent through these pseudowires to drop.

  In the failed state, the router has the following symptoms:

  1. the following command shows packets dropped in the Disabled row:

```
1k-60-2#sh pl ha qfp act stat drop clea | ex _0_
-----------------------------------------------------------------
Global Drop Stats                        Packets        Octets
-----------------------------------------------------------------
  Disabled                              48770         3627820
```

  2. the following command shows some ATM interfaces have packet drop:

```
1k-60-2#sh platform ha q act int all stat dr su cl
-----------------------------------------------------------------
Drop Stats Summary:
note: 1) these drop stats are only updated when PAL
         reads the interface stats.
```

```
Interface                                             Rx Pkts            Tx Pkts
------------------------------------------------------------------------------
ATM0/1/0.378                                             1518                  0
ATM0/1/0.422                                             1518                  0
ATM0/1/0.1129                                             824                  0
```

3. the following command shows that no xconnect configure on the affected ATM interface in qfp side:

```
1k-60-2#show plat hard qfp act feat xcon cl int ATM0/1/0.1129
 % Error: Unable to get xconnect config interface=ATM0/1/0.1129
```

4. **sh platform software atom fp active xconnect** shows fewer entries than **sh platform software atom rp active xconnect**.

```
1k-60-2#sh platform software atom fp active xconnect
ATOM/Local Cross-connect table, Number of entries: 7712

1k-60-2#sh platform software atom rp active xconnect
Number of xconnect entries: 7736
```

The root cause of the issue is when ATM PVC is downloaded to FMAN on the PE router. In addition when XConnect has been downloaded due to the long delay in setting up ATM PVC in IOSD shim layer. The problem only happens with ATMoMPLS, and only when ATM PVC is being set up with XConnect being pre-configured on it. An example scenario is ISSU.

Workaround: There are a couple of workarounds for this issue.

1. When the problem happens, remove xconnect and then add back xconnect on these affected ATM interfaces. You can find out such interfaces with **sh platform ha q act int all stat dr su cl** when traffic is on. Another way is to find the affected interfaces is to run **show plat hard cpp act feat xcon cl int INTERFACE_NAME**. If it has the following sample output while it has xconnect configured in IOS, then it is affected:

```
1k-60-2#show plat hard cpp act feat xcon cl int ATM0/1/0.1129
% Error: Unable to get xconnect config interface=ATM0/1/0.1129
```

2. When the problem happens, run **clear xconnect all,** which will re-provision xconnect. This command may take several miniutes to fully re-provision xconnect on all configured interfaces.

3. To remove xconnect configure before ISSU, and then add it back after ISSU completes.

- CSCtc80502

  On the Cisco ASR 1000 Router the following traceback message has been seen:

  FRR_OCE-3-GENERAL: un-matched frr_cutover_cnt message seen with tracebacks

  This has been observed during ISSU upgrade from 2.4.2 up to 2.5.0 releases.

  Workaround: There is no workaround.

- CSCtc81949

  Service policy application on the standby LNS fails, while its successful on the active.

  If static ip route is configured on the LAC to the l2tp tunnel interface on the LNS, the FIB next hop does not get configured on the standby LNS and hence QOS application fails.

  Workaround: To do a LAC reload to resolve this problem.

- CSCtc85586

  L2TP High Availability (HA) functionality does not work and the standbyRP does not see L2TP sessions.

This happens when the active RP does not have any VPDN/L2TP configuration before the standby RP is brought up.

Workaround: The workaround is to restart the standby RP.

Further Problem Description: This problem can be avoided by configuring "vpdn enable" on the active RP before bringing up the standby RP.

- CSCtc88760

  CPU hog and trace back when using **sh ip bgp vpnv4 x.x.x.x/y** on the Cisco ASR 1000 Router.

  Workaround: None

- CSCtc91594

  High CPU utilization Session churn may happen on the ASR 1000 Router Series.

  Workaround: The following global configuration has helped in reducing the CPU:

  ```
  no parser command serializer
  ip routing protocol purge interface
  ```

  Further Problem Description: CPU will remain high under normal conditions given a constant churn rate of approx 24cps coming up and down.

- CSCtc95423

  Router crashes when quickly unconfiguring and reconfiguring crypto maps on a Cisco ASR 1000 Router.

  This may only occur, when crypto is turned on while SAs are still being deleted in the background and duplicate SAs may be created, which may cause the router to crash.

  Workaround: Before re-applying crypto maps, wait until all SAs on the router are deleted before turning crypto back on.

- CSCtc96161

  DMVPN is working fine for a ~week and then one of spokes appears to be no longer able to pass traffic to other spokes. IPSEC tunnel between the spokes can be established at IOS level, but cannot be programmed into hardware and traffic is not getting through.

  This problem is only seen when there are more spoke to spoke dynamic tunnels and the dynamic tunnels are flapping frequently for a long period of time.

  Workaround: Reduce the frequency of dynamic tunnel flapping by increasing NHRP hold down timer to avoid tearing down dynamic tunnels too often. This can reduce the chance of hitting the problem. But when the problem happens, the affected spoke has to be reloaded.

- CSCtc97134

  GetVPN Fail-Close feature does not work with vrf-lite configuration on the ASR 1000 Router Series.

  This may occur, when Fail-Close map has been configured on vrf.

  Workaround: None

- CSCtc97794

  The ASR 1000 Router Series may crash, while removing encap pppoeoqinq sub interface under traffic.

  This may occur, when removing encap pppoeoqing sub interface with traffic loaded. This condition may Could happen randomly.

  Workaround: None

- CSCtd00479

  When ISIS is configured for NSF IETF, if the restarting router is a DIS on the LAN, then after switchover, the ISIS database and topology could be incorrect. This resulted in incorrect routing table.

  This can occur, when ISIS is configure for NSF IETF and switchover happens.

  Workaround: Is to use NSF CISCO is possible, or disable NSF.

- CSCtd05318

  Watchdog exception crash on “MRIB Transaction”may be observed on a new active RP when RP switchover is initiated.

  This may occur, when RP switchover is triggered under a scaled scenario in the router config with approximately 1K EBGP peers with 500 K Unicast routes and f300 mVRF's with 1K Multicast routes.

  Workaround: None

- CSCtd08733

  On the ASR 1000 Router, when **show hw-module subslot <x/y> entity** returns card-status as partial for 12in1 SPA interface.

  This has been observed when ENTITY-MIB does not have entries for 4XT SERIAL SPA4XT-SERIAL SPA for the main module.

  Workaround: No workaround.

  Further Problem Description: No impact on functionality. The following condition may only occur:

  1. When **show hw-module subslot <x/y> entity** returns card-status as partial.
  2. ENTITY-MIB does not have entries for 4XT SERIAL SPA except main module entity.

- CSCtd16888

  Sessions may hang indefinitely, until the Cisco ASR 1000 Router is rebooted.

  Workaround: None

- CSCtd19446

  The **ip vrf forwarding** command may be disallowed in template mode on the ASR 1000 Router Series.

  Workaround: Is to configure the command without template mode, when possible.

- CSCtd23529

  A LNS doing L2TP HA could reload at l2tp_l2x_session_get_acct/micro_block_get when L2TP sessions are being brought up and a RP switchover is done.

  When RP switchover is being done on LNS while L2TP sessions are being brought up.

  The following error message traceback may be oberved just before the reload:

  %L2TUN-3-ILLEGAL: Error inserting session_socket_db entry, socket_hdl=...

  When a control packet for the session comes in during a very small time window just after this traceback, the router may reload. Since this time window is very small, generally this crash will not be observed after the above traceback.

  Workaround: None.

- CSCtd31638

  When radius-server attribute 31 append-circuit-id is configured for PPPoE, PPPoEQinQ, PPPoEvlan interfaces, nas-port-id should also be appended along with circuit-id.

  This will occur only, when radius-server 31 attribute append-circuit-id is configured.

  Workaround: None.

- CSCtd32406

  The vtemplate interface associated distribute list does not work.

  This may happen, when configuring distribute-list with a vtemplate interface under the router configuration sub mode.

  Workaround: None.

- CSCtd33642

  Flow/Service Accounting records are missing if “delay-star” is configured on a Cisco ASR 1000 Router.

  This may occur, when “aaa delay-start” is configured on the router.

  Workaround: Removing delay-start will result in accounting records generating.

- CSCtd34011

  When a dialer interface configured for PIM goes down, the following message can be seen in the logs every minute:

  %PIM-5-NBRCHG: neighbor 0.0.0.0 UP on interface Dialer1

  Those 0.0.0.0 neighbors will also appear under **show ip pim neighbor** command and will not expire.

  This problem is observed when using a dialer interface configured with PIM.

  Workaround: Is to performing a **shutdown** and then **no shutdown** on the dialer interface clears the 0.0.0.0 neighbor entries.

- CSCtd35091

  The input queue on ISG's access interface gets filled up increasingly causing the interface to wedge. When l2 connected IP session for a client exists on the ISG and traffic from that client comes in with a different IP address than the one used to identify the session, this traffic is dropped and interface wedging is observed.

  Workaround: There is no workaround. A reload of the box is required.

- CSCtd40245

  The Cisco ASR 1000 Router may crash with a traceback pointing to ‘ess_stats_poll_message_create'.

  When FP goes down for any reason, and at the same time PPPoE session goes down or ISG service log off happens, the RP will also crash, after “subscriber accounting accuracy” is configured. This problem is only applicable to release 2.5.0.

  Workaround: Is to remove “subscriber accounting accuracy” configuration.

- CSCtd42366

  Sum of total packet/bytes counts with multiple services logon/logoff may exceed total packages/bytes count of the session. This issue can be seen, when Non-TC service A and Non-TC service B are applied alternatively on a PPPoX session during a session life time. Packets count for service A plus packets count for service B would exceed total packets count for PPPoX session.

With continuous traffic sending to a PPPoX session, Non-TC service A is removed immediately followed by another Non-TC service B (essentially it is the same accounting criteria as service A) or within 10 seconds. Then the session is brought within 10 seconds.

Workaround: Is to apply Service B after 10 seconds then do a Service A removal. Another way to avoid this problem is to install default iedge session accounting. Adding services on top of iedge accounting would not see this issue.

Sum of total packet/bytes counts with multiple services logon/logoff may exceed total packages/bytes count of the session. This issue can be seen when Non-TC service A and Non-TC service B are applied alternatively on a PPPoX session during a session life time. Packets count for service A plus packets count for service B would exceed total packets count for PPPoX session.

With contiguous traffic sending to a PPPoX session, Non-TC service A is removed immediately followed by another Non-TC service B (essentially it is the same accounting criteria as service A) or within 10 seconds. Then the session is brought within 10 seconds.

Workaround: Service B is applied after 10 seconds of Service A removal. Another way to avoid this problem is to install default iedge session accounting. Adding services on top of iedge accounting would not see this issue.

- CSCtd43841

  Two framed-ipv6-prefix are present in accounting stop when following CLI's are enabled:

  aaa accounting include authprofile framed-ip-address

  aaa accounting include authprofile framed-ipv6-prefix

  aaa accounting include authprofile delegated-ipv6-prefix

  The above CLIs are needed when all the following 3 conditions are met:

  1. Dual Stack Server and
  2. “aaa accounting delay-start”is configured and
  3. either ipv4 or ipv6 negotiation fails.

  These CLIs are needed to include the IPv4 and IPv6 attributes in the accounting record sent. Only in such scenario, framed-ipv6-prefix may be present twice in accounting records.

  Workaround: On dual stack server with “aaa accounting delay-start”, need to ensure that both IPv4 and IPv6 negotiation are successful for the accounting records to be sent. In such case, there is no need to include above mentioned CLI's (in symptom).

- CSCtd47813

  Traffic loss may be seen after rekey between the Cisco ASR 1000 Router Series acting as GMs when modifying KS ACL. This may only occur, when a more specific permit statement has been added. In addition, when permit ip any any has been applied this will result in traffic loss when rekeying the router.

  Workaround: Is to keep permit ip any as the last acl in the KS ACL set.

- CSCtd48203

  On a Cisco ASR 1000 Router, after the last cache engine in a WCCP service group goes away, packets start getting dropped instead of being forwarded to original destination.

  This problem occurs when the last cache engine present in a WCCP service group becomes unavailable.

  Workaround: To overcome this problem, remove the global service group definition of the service group whose all CEs have become unavailable by using the following CLI conf t:

```
conf t
 no ip wccp <web-cache | service-group-id>
   (or)
Remove the redirect in config from the interfaces on which the service group is
attached, like
conf t
 int <interface name>
 no ip wccp <web-cache | service-group-id> redirect in
```

- CSCtd50125

  GetVPN on the Cisco ASR 1000 GM fails to download the TEK information in the hardware [debug crypto ipsec output below] *Nov 27 02:20:38.323: IPSEC(download associate flow):

```
flow_info: in_flow_id: 2400005F, out_flow_id 24000060
    out_flow_enable: 0
    acl_line_num 1
    sadb_root_local_add: 172.16.0.1
    local_proxy: , remote_proxy:
    in_spi: 35EB57B0, out_sp
*Nov 27 02:20:43.341: IPSEC(crypto_ipsec_create_transform_sas): Failed to attach
flowid to hw
*Nov 27 02:20:43.342: IPSEC(delete_sa): deleting SA,
  (sa) sa_dest= 172.16.0.1, sa_proto= 50,
    sa_spi= 0xD2A8F435(3534287925),
    sa_trans= esp-aes 256 esp-sha-hmac , sa_conn_id= 2093    sa_lifetime(k/sec)=
(0/115),
  (identity) local= 172.16.0.1, remote= 0.0.0.0,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4)
*Nov 27 02:20:43.342: IPSEC(update_current_outbound_sa): updated peer 0.0.0.0 current
outbound sa to SPI 3751CFC3
*Nov 27 02:20:43.342: IPSEC(delete_sa): deleting SA,
```

  This condition has been observer, when IPv6 configured on the crypto map local address,

  Workaround: Is to disable IPv6 and reload the box.

- CSCtd54611

  The system console may not response on the ASR 1000 Router Series.

  This symptom has been observed on a Cisco ASR 1000 Router Series, when the router functions as an IP Security (IPSec) termination and aggregration router. In addition, when a self-signed cerificate is configured during Forwarding Processor (FP) is out of service on the router.

  Workaround: There is no workaround. The console will be back to service when FP is active, or when the request gets timeout (around 480 seconds).

- CSCtd55219

  Potential traffic loss on NSF switchover on a Cisco ASR 1000 Router.

  The following debug has been observed:

  00:11:31: BGP(base): waited 0s for the first peer to establish

  You should instead see:

  00:03:54: BGP(base): will wait 60s for the first peer to establish

  ^^^^^^^^^^^^

  Workaround: None.

- CSCtd90265

  IP Security (IPSec) functionality stops working. Route Processor (RP) CPU rate can be high.

This symptom is observed on a Cisco ASR1000 series router when functions as an IP Security (IPSec) termination and aggregration router, and when super package In-Service Software Upgrade (ISSU) was performed with IPSec traffic running.

Workaround: There is no workaround.

- CSCte18684

  PPPoE sessions are likely torn down, when user profile contains “lcp:interface-config”.

  This may occur due to pending state returns from virtual-template cloning, when multiple aaa attributes are parsed from lcp:interface-config user profile.

  Workaround: There is no work around when this configuration is applied on a PPPoE Session.

- CSCte29294

  On the Cisco ASR 1000 Router the ESP may crash, when doing High Availibility (HA) switchover during LNS tests.

  This has been seen, when LNS has been configured with traffic.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 2.5.0

This section documents possible unexpected behavior by Cisco IOS XE Release 2.5.0

- CSCsu03501

  BRR across Vlans works fine on the ASR 1000 Router Series. However, BRR error across class queues sharing same logical interface is in the range 8-10%. This can cause throughput drop to a Class Queue, only when total traffic to interface is above line rate

Note

- This is not interface throughput drop. Total interface throughput is normal). This error in CQ brr is within limits for most cases (1PQ/4CQ, 2PQ/4CQ and 2PQ/6CQ). Error in CQ brr for 12CQ and 2PQ is noticeable when total traffic on the interface is above line rate.

  Workaround: None

- CSCsw44668

  Conditional debugs is not complete on the ASR 1000 Router Series. This condition is more likely to happen when debug is enabled on the tunnel, issuing **shut** and then **no shut**.

  Workaround: None

- CSCsx59262

  The OSPF neighbors on ASR 1000 Router Series bounce after changing the config-register. When OSPF interfaces are configured with fast hellos, the OSPF neighbors on ASR 1000 Router Series bounces, when value 'config-register' is changed.

  Workaround: Is to use BFD.

- CSCsx83443

  Iskmp debug messages from all peers are shown in the term monitor enable tty and vty's

  even though **debug crypto condition peer ipv4 x.x.x.x** is set. This is seen on the ASR 1000 Router Series when using peer ip based debug condition,

  Workaround: None

- CSCsz16142

  When ACL sequence is configured on the ASR 1000 Router Series the RP SWO will not change.

  Workaround. None

- CSCsz24691

  Traffic forward rate is incorrect after changing to "match none" for class multiple criteria. When the ASR 1000 Router Series is configured as the following:

```
class-map multiple_criteria
no match ip precedence 2
no match ip dscp 16
no match access-group name multiple_criteria_acl
no match protocol ip
no match not protocol gre
```

  Workaround: Is to remove all filters.

- CSCsz53438

  On the Cisco Systems ASR1000 Router Series, if IP header compression is configured on the ASR 1000, but not on the corresponding router, an unexpected reload of the embedded systems processor may occur.

  This condition occurrs when IPHC is configured on the AR1000 Router Series, but not on the router to which it is directly connected to.

  Workaround: Is to **enable** IPHC on both routers.

- CSCsz66060

  When saving half duplex vrf configuration then rebooting the router, the half duplex vrf configuration does not apply to the ASR1000 Router Series. This is a rare condition that only happens when the router has been rebooted, after saving half duplex vrf configuration.

  Workaround: Is to re-enter the half duplex vrf configuration again.

- CSCta17502

  If shared IPSec profile has been applied on a tunnel interface, then the tunnel source cannot be modified without removing tunnel protection from the interface.

  The basic condition being enforced is that if there are two tunnels sharing the same ipsec shared profile, then their tunnel sources must be the same.

  Workaround: None

- CSCta65347

  CME is changing the media direction attribute as “INACTIVE”instead of “RECVONLY”on the ASR1000 Router Series.

  Only in this instance the resume fails, when CCM/CME scenario's from h323 legcalls are used and there is no media on the ASR 1000 Router.

  Workaround: None

- CSCta76312

  On the ASR 1000 Router Series the console gets stuck.

  This condition only happens when using the following:

  - downloading a huge config,
  - after unconfiguring the config

  - then doing a config replace.

  Workaround: None

- CSCtb07144

  When issuing a shut command an interface that is configured with vlan that has IGMP joined can take about a minute on the ASR1000 Router Series. In this condition the console hangs after issuing the shut command, and the traffic does not stop right away after shutting the interface on the router.

  Workaround: None

- CSCtb13789

  Tracebacks are seen while initiating config and unconfig when dmvpn tunnel is configured on the ASR 1000 Router Series. This condition will happen when using config and unconfig when dmvpn tunnel is configured.

  Workaround: None

- CSCtb24959

  The ASR 1000 Router Series may fail while clearing large number of rp mappings. This instance can happen when the following has occurred:

  - the router has been configured for rp agent and candidate
  - there are a large number of rp's
  - initiating the **clear ip pim rp-map** command

  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: None

- 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.

- CSCtb70115

  Bgp state in the **show ip bgp vpnv4** show command in all of the summaries are in NoNeg state instead of Active and Idle state. This instance happens when the neighbor has no session in established state in any of the address-families.

  Workaround: Is to configure the **show ip bgp vpnv4 all nei <address>** show command

- CSCtb72095

  When the service policy is removed after the vlan has been re-attached, the session policy will be re-parented to the main interface but it will not re-parent back to the subinterfaces. This instance is only seen when there are vlans and sessions configured on the subinterfaces.

  Workaround: There is no workaround for this. The only option is to reload the router back to it's orginally state.

- CSCtb72734

  DHCP OFFER not reaching the client with unicast flag set on the ASR 1000 Router Series. This occurs only on the ASR 1000 Router Series where creation/removal of ARP entry does not maintain sequential ordering as a result packet could arrive at forwarding plane after the ARP entry has already been removed, or before ARP entry has been created.

  Workaround: None

- CSCtb74547

  The ASR 1000 Router Series DMVPN HUB reloads when processing IPSEC key engine.

  This conditions happens when dual DMVPN with shared tunnel protection feature is enabled.

  Workaround: None

- CSCtb75027

  MVPN traffic has been dropped while enabling nat on the core interface using cli “ip nat outside” on the ASR 1000 Router Series. This instance occurs when mVPN and NAT features are configured together on the router.

  Workaround: As of now, there is no workaround . The other option is to remove NAT on the core interface to receive the mVPN traffic.

- CSCtb80765

  The sub-interface flap on the ASR 1000 Router Series may close on the port channels prior to configuring the ATM SPA. This conditon occurs when the sub-interface flap closes, when the port channels prior to configuring the ATM SPA.

  Workaround: None

- CSCtb86811

  On the ASR 1000 Router Series the following error message may state:

  `"%MFI_LABEL_BROKER-3-MULTIPLE_BIND"`
  within Standby mode, after initiating the **configure replace** command.

  This may occur, when there are large vrf scalability configurations, after static routes are in use in conjunction with **encapsulation ppp** and **mpls label mode all-vrfs protocol all-afs per-vrf**.

  Workaround: There is no workaround for this specific command sequence and configuration.

- CSCtb87546

  Tftp server may times out sometimes or always on the ASR 1000 Router Series. This may occur when uploading or downloading files, including IOS images to tftp server.

  Workaround: Is to use 2.5 pre-released images on the router in order to run the tftp operation successfully.

- CSCtb96600

  All new calls dropped after RP2 switcover on ASR 1004 RP2_ESP20 router. This may occur after intiating RP2 switchover when the cli "redundancy force-switchover" happens on the router.

Workaround: None

- CSCtc12334

  The ASR 1000 Router Series may fail when initiating "clear ip bgp " command.

  This command deletes all bgp neighbor relationships and clears bgp RIB.

  This can occur when the following has been configured:

  1. Need to have MDT configured on the router

  2. Need to issue **clear ip bgp** command

  Workaround: None

- CSCtc16232

  When the L2 MAC address of an Ethernet interface is changed on the ASR 1000 Router Series, the final RA is not sent to the remote endpoint.

  The expected behaviour is that when the L2 MAC address is changed, on theASR 1000 Router is to send a final RA to the endpoint indicating the change.

  Workaround: None

- CSCtc17366

  Only 1-way media or no media is passng when call setup is establish on the ASR 1000 Router Series. This may occur when SIP trunk has been configurated or any setup using 2 IP adress pair with sport and dport equals 5060 for multiple dialogs on the router.

  Workaround: There is no straight forward workaround other than to put the call on hold, then resume the call to try and recover the media.

- CSCtc19914

  The Embedded Services Processor (ESP) is reloaded when configuring and unconfigure a large static RP addresses multiple times rapidly with mVRFs on the ASR 1000 Router Series.

  When using the following scripts this condition has been seen:

  1. Configuring large mVRF's 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: None

- CSCtc22109

  The PPPoEoA sessions when established over ATM VP tunnel may time out on the ASR 1000 Router Series. Only in this instance, a problem can occur when PPPoEoA sessions are established over ATM VP tunnel on the router. When when PPPoEoA sessionst are established directly on ATM VC, the sessions works fine.

  Workaround: None.

- CSCtc30420

  CPP tracebacks are logged after configuring the ASR 1000 Series Router as an RP2 with IPSec DMVPN Spoke. Only in this condition, when unconfiguring DMVPN on the router and reconfiguring it again, CPP tracebacks are logged.

  Workaround: Is to reload the router.

- CSCtc33471

  CPUHOG message has been seen indicating MFIB_mrib_read as the offending process after a **clear ip mroute** command is issued on the ASR 1000 Router Series. This conditions happens when there arelarge scaled configurations and there are a huge number of forwarding interfaces on the same multicast forwarding entries.

  Workaround: There is no known workaround.

- CSCtc33511

  When sending very low policing value for the rate, less than 500 bps, from dynamic clients such as Radius, will crash the ASR 1000 Router Series. This condition may happen when a policing rate is set to lower than 500 bps on the router.

  Workaround: None

- CSCtc33821

  IOS may crash when configuring MPLS over Generic Routing Encapsulation (MPLSoGRE) on the ASR 1000 Router Series. Only in this condition, when MPLSoGRE is configured and one GRE tunnel interface is shutdown after the address has been removed and another GRE tunnel is added the IOS may crash on the router.

  Workaround: None

- CSCtc42960

  On the ASR 1000 Router Series memory leaks have been seen when using PPPoX sessions. This may occur when memory leaks have been observed with PPPoX sessions in scaled scenario's.

  Workaround: None

- CSCtc43110

  Under H.323 call scenarios, outgoing H.323 signaling packets (TCP) are marked with a non-zero DSCP value, even though no QoS is configured for H.323 calls. This happens under all H.323->H.323 and SIP->H.323 scenarios when SBC creates a downstream H.323 calls.

  Workaround: There is no workaround with SBC configuration. QoS can be re-marked when MQC policy is placed on the outbound physical interfaces of the ASR 1000 Series Router. ASR 1000 Series Router. CSCtc44472

  After SSO of the RP with 660 VRF aware NAT configuration the FP crashes on the ASR 1000 Router Series. This conditions happens when RP has VRF and NAT configured on the router.

  Workaround: None

- CSCtc52358

  When a previous "logging buffer" is done on the ASR 1000 Series Router as subsequent cli is on .

  Workaround: Is to do another "logging buffer" the the previous one will be released.

- CSCtc54042

  The ASR 1000 Router Series may crash 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: None

However if problem manifests, the subsequent rebooting is very likely to be successful. If stuck in a situation where crashes are repetative, momentarily pull redundant RP until system stabilizes, and re-insert redundant RP.

- CSCtc69991

  When the Cisco ASR 1000 Router has been configured as a DMVPN spoke it may throw tracebacks. This can happen when ODR is configured as the Overlay Routing protocol and shut/no shut is done on the tunnel interface.

  Workaround: Is to use eigrp as the overlay routing protocol.

- CSCtc70661

  The ASR1000 Router Series ESP may unexpectedly reload during sequences of repeated configuration change which also cause “flapping” of large numbers of auto-vcs. This may be seen with 4k active auto-vcs when the config on the PVCs is changed from PTA to L2TP multiples times.

  Workaround: None.

  In addition, can be timing related and has been seen so far in cases of scripted config changes from: PTA-> L2TP. It has not been seen in cases of changing the config from PTA-> PTAor from L2TP -> L2TP

- CSCtc71004

  During Change of Authorization (CoA), a message may show that an Access Control List reference

  failed to download. This behaviour may be seen on ASR1000 images where a series of CoA requests rapidly cause

  Traffic Classes to be applied and removed. It may be more likely to happen when there are more

  Traffic Classes applied to a session.

  WorkAround: None

  In addtion, If this message is seen, the session will likely be torn down, and have to be brought back up on the router.

- CSCtc71338

  When configuring a 10k line ACL (production-out) on the interface, the FP process crashes on the ASR 1000 Route Series.

  The production-out will show as follows:

```
interface GigabitEthernet0/3/4
 ip address 1.10.4.1 255.0.0.0
 ip access-group production-out in
 ip access-group production-out out
 speed 100
 no negotiation auto
 cdp enable
 service-policy output test
```

  Workaround: None

- CSCtc72651

  A crash has been seen on a new RP after SSO with AToM debugs are enabled on the ASR 1000 Router Series. When enabling AToM debugs which requests VC Accouting details from MFI during SSO the router may fail.

  Workaround: None

- CSCtc73657

  ASR 1000 Router Series may fail when core file points to the Range Inheritance . This condition may happen, when PVC is locked or PVC teardown Fails in CPP on the router. In addditon, when the Range has been deleted and the PVC has not been removed from the common code.

  The Range's stale pointer should be cleaned up on the router.

  Workaround: None

- CSCtc76353

  ASR 1000 Router Series may fail when core file points to the Range Inheritance . This condition may happen, when PVC is locked or PVC teardown Fails in CPP on the router. In addditon, when the Range has been deleted and PVC will not be removed from the common code . Note: The Range's stale pointer should be cleaned up

  Workaround: None

- CSCtc76598

  MFIB_IPv4 sub-block not removed from virtual access interface on the ASR 1000 Router Series. The error is shown when pppoe session is established on the router.

  Workaround: None

- CSCtc79444

  On the ASR 1000 Router Series config bulk sync failure has been seen.

  This condition may happen, when configuring" static-ipfrr ipv4-nexthop Loopback0 1.1.1.1 backup Loopback1 1.1.1.2" and removing the loopback 0 in current active, followed by doing a first switchover and a sync failure on the router. This is due to the command as being shown as active.

  Workaround: Is to remove the ipfrr static route if the loopback is removed on the router.

- CSCtc80502

  FRR_OCE-3-GENERAL: un-matched frr_cutover_cnt message has been seen with tracebacks on the ASR 1000 Router Series.

  This has been observed during ISSU upgrades starting from release 2.4.2 and up to 2.5.

  Workaround: None

- CSCtc81949

  On the ASR 1000 Router Series Service policy application on the standby LNS fails, while its successful on the active. If static ip route is configured on the LAC to the l2tp tunnel interface on the LNS, the FIB next hop does not get configured on the standby LNS and hence QOS application fails.

  Workaround: Is to reload the LAC resolves the problem.

  CSCtc85586

  L2TP HA functionaity may not work and STANDBY is not seen with L2TP sessions on the ASR 1000 Router Series. This condition may happen, when ACTIVE does not have any VPDN/L2TP configuration before

  STANDBY is brought up on the router.

  Workaround: Is to restart STANDBY.

  Further Problem Description:

  This problem can be avoided by configuring "vpdn enable" on the ACTIVE before bringing up STANDBY on the ASR 1000 Router Series.

- CSCtc86490

  Error message stating "Can't install service policy with empty name" is shown on the ASR 1000 Router Series. This condition hay occur, when an invalid service policy is pushed from the DBS on to the VC, the error message is shown and the policy on the VC doesn't fall to the default on the router.

  Workaround: None.

- CSCtc90996

  While under load for extended periods of time, a condition may ocurr that causes a large amount of stale call legs to exhibit on the ASR 1000 Router Series. These stale call legs can consume enough memory on the platform to cause a crash due to memory outage. It has been observed with 2000 active calls at 20 CPS for an extended period of time.

  Workaround: To avoid a runaway condition, the use of the command max-conn on the dial-peers of the platform is capable of holding back the amount of stale call legs. While the condition occurs that triggers the event, max-conn has the side effect of not permitting calls to be established over this dial-peer. Eventually it will clear and calls may continue.

- CSCtc96161

  DMVPN is working fine for a week and then one of spokes appears to be no longer able to pass traffic to other spokes. IPSEC tunnel between thespokes can be established at IOS level, but cannot be programmed into hardware and traffic is not getting through. This problem is only seen when there are more spoke to spoke dynamic tunnels and the dynamic tunnels are flapping frequently for a long period of time.

  Workaround: Is to reduce the frequency of dynamic tunnel flapping by increasing NHRP hold down timer to avoid tearing down dynamic tunnels too often. This can reduce the chance of hitting the problem. But when the problem happens, the affected spoke has to be reloaded.

- CSCtd00644

  The ASR 1000 Router Series may restart ungraceful with scaled config. When there is scaled config and sessions are flapping frequently, only on rare instances the ASR 1000 Router Series may restart ungracefully. This problem may also timing related, so it may not happen with every time sessions flaps.

  Workaround: None

- CSCtd05318

  Watchdog exception crash on “MRIB Transaction” may be observed on a new active RP when RP switchover is initiated on ASR 1000 Series Router. This happens when a RP switchover Trigger under a scaled scenario of router config with approximately 1K EBGP peers with 500 K Unicast routes + 300 mVRF's with 1K Mcast routes.

  Workaround: None

- CSCtd14048

  After ISSU loads the 2.5 images, ISG PPPoE Sessions will not be established on the ASR 1000 Router Series. In this conditon there is no ISG PPPoE Session established on the router.

  Workaround: None

- CSCtd17197

  The serial interface with “frame-relay” encapsulation goes down and can no longer forward traffic, when “keepalive” is configured along this interface. The serial interface has both "frame-relay" encapsulation and keepalive configured.

Workaround: Configure “no keepalive” on the serial interfaces of both sides when we use “frame-relay” encapsulation on the interfaces.

- CSCtd26479

  On ASR 1000 Router Series, the FP may crash with the following error message:

  ```
  %IOSXE-6-PLATFORM: F0: cpp_ha: Shutting down CPP MDM while client(s) still connected
  ```

  The FP crashes may happen in some instances, when switchover is pushing COA toward PPPoE and there are 1000 PPPoE ISG sessions on the router.

  Workaround: None

- CSCtd32560

  During Cisco ASR 1002 or Cisco ASR 1004 ISSU upgrades from 2.3.2 to 2.5, observed loss of QoS functionality. This condition happens when loss of QoS functionality has been observed right after CC/SPA upgrade, while following Cisco ASR 1002 or Cisco ASR 1004 ISSU procedure.

  Workaround: Is to reverse the order of CC/SPA and FP upgrades so that FP will be running 2.5.

  when CC/SPA is upgraded to 2.5.

  ISSU procedure for this workaround will be:

  1. Upgrade the RPAccess, RPIOS, and RPControl sub-packages in the standby bay. Once the SSO state is reached, commit the software version.

  ```
  issu loadversion rp 0 file file-system:asr1000rp1-
  {rpaccess,rpios,rpcontrol}*version-string*.pkg bay standby-bay force
          issu commitversion
  ```

  2. Force a switchover from the active IOS process to the standby IOS process.

  ```
  redundancy force-switchover
  ```

  3. Upgrade the RPAccess, RPIOS, and RPControl sub-packages in the standby bay (a different bay than in step 1). Once the SSO state is reached, commit the software version.

  ```
  issu loadversion rp 0 file file-system:asr1000rp1-
  {rpaccess,rpios,rpcontrol}*version-string*.pkg bay standby-bay force
          issu commitversion
  ```

  4. Upgrade the ESP Base sub-package and Commit the ESP Base software

  ```
  issu loadversion rp 0 file file-system:asr1000rp1-esp*version*.pkg
  force
          issu commitversion
  ```

  5. Upgrade the SIP and SPA sub-packages for each SIP on the router.Repeat this step for each SIP installed in your router before proceeding to the next step.

  ```
  issu loadversion install rp 0 file file-system:asr1000rp1-
  {sipbase,sipspa}*version*.pkg slot SIP-slot-number force
          issu commitversion
  ```

  6. Upgrades all sub-packages, including the RPBase sub-package, which is the last sub-package that needs to be upgraded

  ```
          issu loadversion rp 0 file file-system:asr1000rp*version*.pkg
  ```

  7. Verify that the sub-packages are properly installed

  ```
  show version installed
  ```

  8. Reload the RP. The router will continue normal operation even without a reload, so you can reload the router during scheduled maintenance or a slower traffic period.

  ```
  reload
  ```

- CSCtd34284

  ASR 1000 Router Series is experiencing this error message on the console:

```
 %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:00 Thread:100 TS:00000016373874688294
%QOS-3-INVALID_CLASS_QID:
```

When the router is receiving COA in the background after a switchover.

Workaround: None

- CSCtd34644

  Hub and spoke on the ASR 1000 Router Series in DMVPN - Hub Support by QoS Class (DMVPN Phase 3) the network shows ATTN SYNC timeout and IPSEC-3-CHUNK_DESTROY_FAIL messages in steady state traffic and during dmvpn config cleanup. This is seen during scale config and configuration cleanup.

  Workaround: No Workaround

- CSCtd38347

  CPP can run out of memory and cause FPs to reload on the ASR 1000 Router Series. This condition can happen, when flapping LNS firewall sessions are running over time on the router.

  Workaround: None

- CSCtd39409

  IOSD crash on the ASR 1000-WATCHDOG: Process = L2TP mgmt daemon has been seen on the ASR 1000 Router Series.

  This condition has been seen, when flapping on LNS firewall sessions over time happens on the router.

  Workaround: None

- CSCtd42366

  Acct_Input_Packets for non-TC service are inaccurate post CoA for short lived session on the ASR 1000 Router Series.

  On the ASR 1000 Router Series where continuous traffic is being sent using an IXIA, when bringing up a PPPoX session using the dialer interface. The PPPoX session activates 2 TC and 1 non-TC service. After waiting for a few seconds, we perform a CoA-SVC_logon to a new non-TC service. This unapplies the previous non-TC service. We let the session remain up for a few more seconds, before tearing down the session. At this time, when we compare the Rx stats on the IXIA with the Acct_INput_Packets in the account records of the non-Tc services, the Acct-Input-Packets are incorrect.

  Workaround: None

- CSCtd43841

  Two framed-ipv6-prefix are present in accounting stop when following CLI's are enabled on the ASR 1000 Router Series:

  ```
  aaa accounting include authprofile framed-ip-address
  aaa accounting include authprofile framed-ipv6-prefix
  aaa accounting include authprofile delegated-ipv6-prefix
  ```

  The above CLIs are needed when all the following 3 conditions are met:

  1. Dual Stack Server and
  2. “aaa accounting delay-star” is configured and
  3. either ipv4 or ipv6 negotiation fails.

  These CLIs are needed to include the IPv4 & IPv6 attributes in the accounting record sent. Only in such scenario, framed-ipv6-prefix may be present twice in accounting records.

  Workaround: Is to do the following:

On dual stack server with “aaa accounting delay-start”, need to ensure that both IPv4 and IPv6 negotiation are successful for the accounting records to be sent. In such case, there is no need to include above mentioned CLI's (in symptom).

- CSCtd44755

  The ASR 1000 Router Series with ATM SPA, following ERR message is seen on standby RP:

  ```
  Nov 21 15:57:24.192: %ATM-3-FAILCREATEVC: ATM failed to create VC(VCD=1874, VPI=1,
  VCI=1905) on
  Interface ATM0/0/0.65000, (Cause of the failure: VCD# mismatched on standby-RP -reload
  standby-RP)
  ```

  The ASR 1000 Router Series with ATM SPA having 32k pvc-in-range VCs configured with 32k PPPOE sessions and when these sessions are brought down followed by un-configuration of all 32K VCs in below sequence:

  1. Un-configure pvc-in-range.
  2. Un-configure range.
  3. Un-configure sub-interface.

  Workaround: Is to do the following:

  ATM range VC configuration can be removed by just removing the sub-interface alone which has range VC configuration instead of removing it in above mentioned sequence.

- CSCtd44966

  On ASR 1000 Router Series with ATM SPA, one may see following ERR message in fman-fp_F0-0/1.log:

  ```
  [aom]: (ERR): Unable to find async context for AOM
  ```

  On ASR 1000 Router Series with ATM SPA, when ATM VC modify is involved and there are multiple parameters to be modified, one may see such error message in fman-fp_F0-0/1.log

  Workaround: None

Release 2.4 Caveats

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

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

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

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

This section consists of the following subsections:

Open Caveats—Cisco IOS XE Release 2.4.4

This section documents possible unexpected behavior by Cisco IOS XE Release 2.4.4.

- CSCsv66827

  When clearing the SSH sessions from a VTY session causes the ASR 1000 Router Series to crash.

  Workaround: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.

  There are no known workarounds.

- CSCsz01980

  The RP1 may experience unexpected watchdog timeout and reload.

  Under very rare conditions, an RP1 may experience a watchdog timeout during boot or shutdown and subsequently generate a kernel core dump.

  Workaround: No known workaround; following reload, the RP works as expected.

- CSCsz21624

  When doing **no router ospf** a message similar to the following may be seen:

```
%IPRT-3-NDB_STATE_ERROR: NDB state error (BAD EVENT STATE) (0x0) 10.10.10.3/32, state
7, event 0->4, nh_type 1 flags 4 -Process= "OSPF-1 Router", ipl= 0, pid= 268
```

The following conditions have been observed:

1. When there are significant number of IGP routes.
2. An interface has OSPF configured on a Cisco ASR 1000 Router, while running and comes up, when cleanup of the OSPF process is in progress.

Workaround: Is to remove any **network** statements in OSPF before removing the OSPF instance.

- CSCsz47878

  When provisioning LI tap with the same session ID when Radius has been configured on a Cisco ASR 1000 Router, there is a chance that traceback is observed.

  This condition has been observed when an invalid provision of LI tap is used. A unique session ID should be used for each session provisiioning.

  Workaround: Is to use a unique session ID for each session to be provisioned.

- CSCsz62927

  Sometimes header-compression commands may disappear from the configuration after reload has happened on a Cisco ASR 1000 Router.

  This condition has been seen when the following commands seems to be disappear after reload:

  ip rtp header-compression ip tcp header-compression

  Workaround: None

- CSCsz83305

  L2TP tunnel resync duration on a Cisco ASR 1000 Router is observed to be significantly longer an RP2 Route Processor compared to an RP1 Route Processor. For example, around 90 seconds on an RP2 vs 30 seconds on an RP1 for the same number of tunnels (12 000).

  This condition has been observed when the scaling numbers reached over 24k sessions and 12k tunnels.

  Workaround: None

- 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 commmands **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 can occur on any Cisco ASR 1000 Router when 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.

- CSCta35043

  There are numerous amount of chunk leaks observed when using **tcl scripting** commands on a Cisco ASR 1000 Router. This condition has been seen when configuring and unconfiguring the **tcl scripting** related commands, numerous chunk leaks are observed.

  Workaround: None

- CSCta37670

The ASR 1000 Router crash as a longer interrupt hold, when a single MPLS scales up to 300K prefixes.

This instance occurs only when a single MPLS with 300K prefixes. The issue does not occur with 100 prefixes.

Workaround: Is not to run 300 prefixes.

- CSCtb13902

  Password encryption with **key config-key** command on one end of tunnel results in IPSec session to fail.

  This condition has been with a back to back router running IPSec6.

  Workaround: None

- CSCtb30072

  With a 1K DMVPN spoke, if you un/re-configure tunnel protection several times and un/re-configure tunnel interface may reset both Embedded Services Processors (ESPs).

  Workaround: After unconfiguring a tunnel interface with 1K DMVPN spoke, wait for a few seconds before reconfiguring the same tunnel interface with same DMVPN configuration.

- CSCtb37274

  If billing is enabled with a valid cache path as part of the SBC configuration, and records are being written to a removable device, such as a USB drive, and the device is removed from the router, an unexpected system reload can occur.

  This issue occurs if billing records are being written to a removable device and while operations are active, the device is removed from the router. Upon replacing the device and attempting to deactivate billing, an unexpected system reload occurs.

  Workaround: To avoid this issue, do not remove the device billing records are cached to while records are being processed.

- CSCtb49373

  When static route is pointing to next-hop (without exiting an interface)this does NOT get removed from the routing table when route towards next-hop disappears on the ASR 1000 Router Series.

  This condition may occur when there is a less specific static route including the prefix of the static route are not removed.

  Workaround: Is to specify an exit interface in addition of next-hop.

- CSCtc45832

  When tracking stops the data-plane logs out of the PKT-MEM trace log this problem will occur on the ASR 1000 Router Series the sessions will be dropped and the QoS hierarchy will shut down. There also will be pending queue objects waiting to be flushed out in the list.

  The following command will show the BQS RM status:

  show plat hard qfp act inf bqs stat

  In rare conditions, an error may occur for extreme over-subscribed enviroments. When sending 10G (For example: 5G as priority, and 5G as non-priority) traffic to a 1G interface.

  All priority and control packets are dropped by the hardware this occur when the packet buffers are depleted; and when the schedule stops forwarding output packets

  Workaround: There is no known workaround to this problem.

- CSCtd58836

When changing DMVPN tunnel source this may result in having hung sessions on a Cisco ASR 1000 Router.

This condition has been seen when the Cisco ASR 1000 Router Series is running IOS XE 2.4 and up to 12.2(33)XND2.

Workaround: Is to shutdown the tunnel interfaces before changing their physical source interfaces.

- CSCtd75807

  OSPF route convergence may be slow when a large number of prefixes are to be downloaded to the ESP.

  This condition may only occur when using RP1 and ESP-10 blades.

  Workaround: There is no workaround.

- CSCte81385

  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, 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.

- 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.

- 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: None

- CSCte97907

  On a Cisco ASR 1000 Router with 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: None

Resolved Caveats—Cisco IOS XE Release 2.4.4

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.4.4

- CSCsw67249

  When a Cisco ASR 1000 Router is acting as a relay, a request for an IP address from a DHCP client fails when the DHCP client is set to unicast.

  This symptom is observed when DHCP clients and the DHCP server are in the same VRF and the DHCP clients are set to unicast.

  Workaround: If the DHCP clients allow it use broadcast method.

  Workaround: There is no workaround.

- CSCsx66105

  Chunk memory leaks at **SADB SA Header** are seen on a Group Domain of Interpretation (GDOI) group member.

  This symptom is observed when IPsec security associations (SAs) are cleared using the command **clear crypto gdoi**.

  Workaround: There is no workaround.

- CSCsy23839

  On Cisco ASR 1000 Router Series, CPU utilization of SIP (SPA Interface Processor) may be 100%.

  This symptom is observed with the following procedure:

  1. Open a terminal window for telnet to ASR 1000.
  2. Telnet to ASR 1000.
  3. Run the request platform software console attach x/x (login SIP IOS) command.
  4. Close the terminal window without exiting from SIP IOS.
  5. You can see that the ioscon process is not terminated and its CPU utilization is around 100% by the monitor platform software process command.

  Workaround: Resetting the SIP resolves the issue.

- CSCsz83570

  SSH sessions disconnect during large data exchanges, such as large logs with pagers.

  The symptom is observed when large amounts of data are exchanged between both ends: client and server (i.e.: the client provides a large input to the server and the server has a large output to send to the client). The session gets hung momentarily and disconnects after the timeout period of 120 seconds.

  Workaround: Use 3DES for encryption.

- CSCta23902

  On a DMVPN router, when the IPSec SAs are deleted, the NHRP holdtime is set to be 5 seconds. This 5 seconds gap between IPSec and the corresponding NHRP cache entry could cause the spoke to spoke tunnel to bounce under certain timing conditions.

  This symptom only occurs under certain timing conditions.

  Workaround: There is no workaround.

- CSCta46347

Connecting a 2 or 4 port OC48 POS SPA{SPA-2XOC48-POS/RPR or SPA-4XOC48-POS/RPR} back to back with either 1, 2 or 4 port OC48 POS SPA{SPA-2XOC48-POS/RPR or SPA-4XOC48-POS/RPR or SPA-1XOC48-POS/RPR} could push the corresponding POS inteface into down/down with SLOS.

This symptom is a timing related issue and could be triggered with the following sequence of operations:

1. Insert the 2 or 4 port OC48 SPA{SPA-2XOC48-POS/RPR or SPA-4XOC48-POS/RPR} without any cable connected.
2. Connect the cables.
3. Do 'no shut' (enable) on the ports.

This could result in the POS interfaces being stuck in SLOS.

Workaround: Enable (do no shut) the ports before fiber is connected.

- CSCtb79600

  IPSec tunnel does not come back up after issuing the **clear crypto session** command at the hub.

  This symptom is observed when bringing up a 2547oDMVPN (RFC 2547) network with one hub and one spoke, and the **clear crypto session** command is issued at the hub.

  Workaround: Issue the **clear crypto session** command at the spoke.

- CSCtc14197

  The following Traceback is seen on the router console following which FP reloads:

```
*Sep 23 09:37:04.432 UTC: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp:  cpp_cp encountered an
error -Traceback= 1#3c307  1031ab84e4601e29a1edaf6b55a   errmsg:D976000 1C00
cpp_common_os:E0C6000 B7C0 cpp_common_os:E0C6000 18B78 cpp_exmem_mgr:ED34000 894C
cpp_wccp_svr_lib:F5DB000 E508 cpp_wccp_svr_lib:F5DB000 107AC cpp_wccp_svr_lib:F5DB000
ACB0 cpp_wccp_svr_lib:F5DB000 7368 cpp_common_os:E0C6000 10618 cpp_common_os:E0C6000
1097C evlib:DD2D000 DBA4 evlib:DD  2D000 FED4 cpp_common_os:E0C6000 11F18 :10000000
3DD0 c:BE2D200 1D078
This symptom is observed when WCCP is un-configured in a specific fashion:
ip wccp 61
ip wccp 62
interface gigabitEthernet 1/3/2
       ip wccp 61 redirect in
       ip wccp 62 redirect in
no ip wccp 62
no ip wccp 61
interface gigabitEthernet 1/3/2
      no  ip wccp 61 redirect in
      no ip wccp 62 redirect in
```

  Workaround: Un-configure WCCP by removing the service applied on the interface first and then removing the global wccp configuration:

```
interface gigabitEthernet 1/3/2
      no  ip wccp 61 redirect in
      no ip wccp 62 redirect in
no ip wccp 61
no ip wccp 62
```

- CSCtc24940

  Tracebacks are seen when crypto profile is applied when L2TP sessions are being brought up.

  This symptom is observed when a crypto profile is not defined and applied to vpdn-group while sessions are being brought up.

Workaround: There is no workaround.

- CSCtc61038

  Tracebacks are seen after removing and adding the Web Cache Communication Protocol (WCCP) service.

  This symptom is observed while traffic is flowing through the router.

  Workaround: There is no workaround.

- CSCtc79484

  Statistics for max-entries limit are not shown.

  This symptom is observed for ASRNAT under all conditions.

  Workaround: There is no workaround.

- CSCtc87430

  The following errors are seen on Active RP during RP switchover with scaled sessions (around 5k):

  asr1000 bsess: RPC header processing failed, error=5001.

  This symptom is observed when the setup is:

  Agilent---(atm)---MCP----(10GB)-----LNS(c10k)-----Agilent

  and the steps followed are:

  1. Configure MCP as LAC with Model D2.1 QOS
  2. Start session bring-up
  3. At aroung 5k session, issue RP swo4. Noticed errors on new Active RP

  Workaround: There is no workaround.

- CSCtc91560

  High CPU utilization occurs.

  The symptom is observed with session churn.

  Workaround: There is no workaround.

- CSCtd00489

  A traceback indicating that the object was being deleted before the ideal exponent is invalidated is logged.

  This symptom is observed while an ATM VC schedule is being deleted. A schedule object is freed before its ideal exponent is invalidated. This condition is treated as an error because it points to a missing step in cleaning up prior to destroying an object since it could potentially impact the rate accuracy in the future.

  Workaround: There is no workaround.

- CSCtd05011

  A buffer overflow can occur which does not have a known impact on router behavior, but may result in a potential memory access violation.

  This symptom occurs when the random number generator function is triggered.

  Workaround: There is no workaround.

- CSCtd21590

  RP crashes after executing no import ipv4 unicast map filter command.

This symptom is observed when BGP import events debugging is on with debug ip bgp import updates or debug ip bgp import event.

Workaround: Do not enable debug ip bgp import event or debug ip bgp import update.

- CSCtd22064

  An ASR 1000 Router Series will crash when removing SBC configuration after a failover.

  During normal call operations a failover is initiated via CLI. Normal call operations continue without issue after the failover. After stopping all calls, the SBC configuration is removed and the ASR 1000 will crash.

  Workaround: Do not remove SBC configuration.

- CSCtd25664

  1. ERSPAN session are not sending traffic to the analyser.
  2. ERSPAN session are not filtering traffic as expected on the router.

  This condition has been observed, when the Cisco ASR 1000 Router is running 12.2(33)XND1 and previous versions.

  1. ERSPAN configured with vlan filtering
  2. ERSPAN configured with vlan sourcing

  Workaround:

  1. Filter traffic on the analyser.
  2. There is no known workaround.

- CSCtd38347

  CPP can run out of memory and cause FPs to reload.

  This symptom is observed when flapping LNS firewall sessions are running over time on the router.

  Workaround: There is no workaround.

- CSCtd61194

  When configuring ERSPAN on FastEthernet, gives an error:

  SPAN is not supported on SPA interface

  ```
  ASR1K(config-mon-erspan-src)#source interface ?FastEthernet FastEthernet IEEE
  802.3GigabitEthernet GigabitEthernet IEEE 802.3z Port-channel Ethernet Channel of
  interfaces TenGigabitEthernet  Ten Gigabit Ethernet
  ASR1K(config-mon-erspan-src)#source interface fastEthernet 0/3/0 SPAN is not supported
  on SPA interface (FastEthernet0/3/0)ASR1K(config-mon-erspan-src)#
  ```

  This symptom is observed on Cisco ASR 1000 Router Series running Version 2.4.1 of Cisco IOS XE.

  Workaround: Configure ERSPAN on GigabitEthernet.

- CSCtd68955

  FMAN-FP may crash with netflow configuration.

  This symptom is observed on ASR1000 Router Series with enabled 2k interfaces, with full and sampled netflow in both ingress and egress direction, and router boot up with netflow configuration.

  Workaround: There is no workaround.

- CSCtd72416

  An error message with a traceback is observed on the router console in the format:

```
%FRAG-3-REASSEMBLY_DBG: Reassembly/VFR encountered an error: VFR failed at refrag:,
first fragment length 370, non-first frag total length 608.
```

The length values may change depending on the actual fragmented packets received by the router.

This symptom is observed when the IP Virtual Reassembly (VFR) feature is enabled on the interface that receives malformed fragmented packets. VFR drops such problem packets as they cannot be correctly processed and generates the error message as a warning.

Workaround: Disable the source of the malformed fragments or disable VFR feature. There is no other workaround.

- CSCtd72441

  On a Cisco ASR 1000 Router Series, when the command **show platform software wccp <*service-id*> counters** is executed, the obj_id field in the output in rare situations may be a large negative number. This is a cosmetic issue and does not affect functionality.

  This symptom is observed when:

  1. WCCPv2 is configured on the router and is redirecting traffic.
  2. The object id value is greater that 2147483647.
  3. The command **show platform software wccp <*service-id*> counters** is executed.

  Workaround: There is no workaround.

- CSCtd75033

  Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability.

  Note Note: The fix for this vulnerability has a behavior change affect on Cisco IOS Operations for Mode 7 packets. See the section Further Description of this release note enclosure.

  Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

  ntp master <*any following commands*>

  ntp peer <*any following commands*>

  ntp server <*any following commands*>

  ntp broadcast client

  ntp multicast client

  The following example identifies a Cisco device that is configured with NTP:

  ```
  router#show running-config | include ntp
  ntp peer 192.168.0.12
  ```

  The following example identifies a Cisco device that is not configured with NTP:

  ```
  router#show running-config | include ntp
  router#
  ```

  To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the show version command to display the system banner. The system banner confirms that the

  device is running Cisco IOS Software by displaying text similar to “Cisco Internetwork Operating System Software” or “Cisco IOS Software.” The image name displays in parentheses, followed by “Version” and the Cisco IOS Software

release name. Other Cisco devices do not have the show version command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
 Cisco Internetwork Operating System Software
 IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
 Technical Support: http://www.cisco.com/techsupport
 Copyright ) 1986-2008 by cisco Systems, Inc.
 Compiled Mon 17-Mar-08 14:39 by dchih
 <output truncated>
```

The following example shows a product that is running Cisco IOS Software

release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version
12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link:

http://www.cisco.com/warp/public/620/1.html

Workaround: There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Note Note: NTP peer authentication is not a workaround and is still a vulnerable configuration.

*** NTP Access Group**

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

```
!--- Configure trusted peers for allowed access
access-list 1 permit 171.70.173.55
!--- Apply ACE to the NTP configuration
ntp access-group peer 1
```

For additional information on NTP access control groups, consult the document titled "Performing Basic System Management" at the following link:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

*** Infrastructure Access Control Lists**

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks.

Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: Network Time Protocol (NTP)
!---
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
 INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
!--- Note: If the router is acting as a NTP broadcast client
!---   via the interface command "ntp broadcast client"
!---   then broadcast and directed broadcasts must be
!---   filtered as well.  The following example covers
!---   an infrastructure address space of 192.168.0.X
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 255.255.255.255 eq ntp
!--- Note: If the router is acting as a NTP multicast client
!---   via the interface command "ntp multicast client"
!---   then multicast IP packets to the mutlicast group must
!---   be filtered as well.  The following example covers
!---   a NTP multicast group of 239.0.0.1 (Default is
!---   224.0.1.1)
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 239.0.0.1 eq ntp
!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.
access-list 150 deny udp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations.  Permit all other traffic to transit the
!--- device.
access-list 150 permit ip any any
!--- Apply access-list to all interfaces (only one example
!--- shown)
interface fastEthernet 2/0
 ip access-group 150 in
```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control List" presents guidelines and recommended deployment techniquesfor infrastructure protection access lists and is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

*** Control Plane Policing**

Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, whilst the second looks at rate limiting NTP traffic to the box.

– Filtering untrusted sources to the device.

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses.

Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```
!--- Feature: Network Time Protocol (NTP)
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD any eq 123
!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.
access-list 150 permit udp any any eq 123
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
class-map match-all drop-udp-class
 match access-group 150
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
policy-map drop-udp-traffic
 class drop-udp-class
 drop
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
control-plane
service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function.

– Rate Limiting the traffic to the device

The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

Warning **Warning: If the rate-limits are exceeded valid NTP traffic may also bedropped.**

```
!--- Feature: Network Time Protocol (NTP)
access-list 150 permit udp any any eq 123
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
class-map match-all rate-udp-class
match access-group 150
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
```

```
!--- for more information on choosing the most
!--- appropriate traffic rates
policy-map rate-udp-traffic
class rate-udp-class
police 10000 1500 1500 conform-action transmit
exceed-action drop violate-action drop
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
control-plane
 service-policy input drop-udp-traffic
```

Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S - Control Plane Policing” at the following links:

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

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

Further Description: Cisco IOS Software releases that have the fix for this Cisco bug ID, have a

behavior change for mode 7 private mode packets.

Cisco IOS Software release with the fix for this Cisco bug ID, will not process NTP mode 7 packets, and will display a message “NTP: Receive: dropping message:

Received NTP private mode packet. 7” if debugs for NTP are enabled.

To have Cisco IOS Software process mode 7 packets, the CLI command <cmd>ntp allow mode private</cmd> should be configured. This is disabled by default.

This is the same as the vulnerability which is described in:

http://www.kb.cert.org/vuls/id/568372

Cisco has release a public facing vulnerability alert at the following link:

http://tools.cisco.com/security/center/viewAlert.x?alertId=19540

Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE and 15.0(1)M.

All other versions of Cisco IOS and Cisco IOS XE Software are affected.

To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returnseither of the following commands listed then the device is vulnerable:

- CSCtd83822

  Increasing memory usage of **reflector.sh** and **droputil.sh** process.

  Workaround: There is no workaround.

- CSCte05713

  The command **sh crypto map gdoi fail-close** has incorrect output.

  Workaround: There is no workaround."

- CSCte08145

  CPP reset after sending malformed GRQ.

  This symptom is observed where an ASR 1000 Router Series is performing ALG. The CPP will reset after some time period.

  Workaround: There is no workaround.

- CSCte38945

  Unable to get ping reply from the multicast group configured on loopback interface.

  The symptom can occur when there are multiple routes populated in an interface and the interface goes down. All the routers associated with the interface should be removed, but only one is deleted. This results in the ping failure.

  Workaround: Shut down the other interfaces associated with the router and enable it again.

- CSCte43708

  QFP crash on ASR 1000 Router Series.

  This symptom is observed when QFP is forwarding an IP fragment while doing IP virtual-reassembly, which is enabled by NAT.

  Workaround: There is no workaround.

- CSCte50144

  Router reports incorrect CPU utilisation. It reports a low CPU utilisation and also reports an overall utilisation lower then the utilisation under interrupts.

  For example:

  ```
  CPU utilization for five seconds: 5%/25%; one minute: 8%; five minutes: 8%
  ```

  This symptom is observed on an ASR1002 router under high CPU utilisation of the RP CPU, caused by excessive rate of punted traffic.

  Workaround: There is no workaround.

- CSCte50721

  During stateful NAT sync of H323 information from primary to standby, standby crashes.

  This symptom is observed on an ASR 1000 Router Series with dual RP and ESP.

  Workaround: Disable H323 with the following commands if H323 ALG is not required:

  no ip nat service h225

  no ip nat service ras

- CSCte51959

  QFP validates the ICMP checksum of all ICMP packets received to a local address even when we ping with 'validate reply data=no'.

  Workaround: There is no workaround.

- CSCte56627

  1. Sessions may not be synchronized properly to standby.

  OR

  2. Session deletes may not be synchronized properly to standby (session that should be deleted on standby, will not be deleted).

  Symptom 1 is observed on ASRNAT when there is an inside mapping and outside static mapping configuration.

  Symptom 2 is observed when a very high burst of session aging occurs.

  Workaround: There is no workaround.

- CSCte57362

FP reset on sending h323 V5 calls via ASR 1000 Router where ASR 1000 is configured with the NAT.

V5 h323 calls should go through ASR-NAT.

Workaround: There is no workaround.

- CSCte60069

  During the scale testing with ModelF applied on PTA, reparenting operation results in FP crash. Also CPUHOG and TIMEHOG tracebacks observed.

  This symptom is observed after the following steps:

  1. PTA: Bring up 24K IPv4 sessions, 2PQ+2CQ(modelf)
  2. Remove grandparent shaper
  3. Add the shaper back.

  Workaround: Avoiding reparenting with large number of vlans/sessions."

- CSCte64646

  A ucode interrupt occurs which causes a driver lockdown.

  This symptom is observed with QoS applied and traffic flowing, when random-detect AND fair-queue are configured in any class, and random-detect is removed from the class (on-the-fly).

  Workaround: If the problem occurs, the FP/ESP must be rebooted. To avoid the problem, stop all traffic or remove the QoS policy from the interface first, then modify that class, then re-apply QoS or restart the traffic.

- CSCte69621

  Missing CLI for configuring deny policy options. “crypto ipsec ipv4-deny {clear|deny|jump}”

  Workaround: There is no workaround."

- CSCte72128

  After a reload, “cdp enable” is missing on previously configured interfaces.

  This symptom is observed on ASR 1000 Router Series running 12.2(33)XNE1, with “cdp enable” configured on some interfaces prior to a reload. After the reload the running-config shows “cdp enable” missing on the previously configured interfaces.

  Workaround: After a reload, manually reconfigure cdp enable."

- CSCte72288

  After changing source VLAN on the source ERSPAN session to a non-existant VLAN or native VLAN (1), traffic is still being received on the SPAN port.

  This symptom is observed on ASR 1000 Router Series with VLANS on a 1Gig port as well as FE port.

  Workaround: There is no workaround."

- CSCte77136

  CLNS routing over GRE tunnels is not working on the ASR 1000 Router.

  This symptom is observed on ASR 1000 Router Series where CLNS routing over GRE tunnels is configured with a GRE tunnel as the egress interface (output from the ASR1000). In this scenario, CLNS packets are not forwarded via fast switching.

  Workaround: Use the following configuration change (needed on a per interface basis):

  “no clns route-cache” to **disable** CLNS fast switching.

- CSCte77167

  Memory leak is observed in QFP, ESP. ESP is also observed to reload after 30hrs of flapping IPv6 sessions

  This symptom is observed on ASR 1000 Router Series with IPv6 session flaps on LNS.

  Workaround: There is no workaround.

- CSCte78589

  FP reload may occur. Crash decode may look like this:

  BackTrace

```
#0  abort () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/logger.c:683
#1  0x8022f779 in rbuf_ooh_handler () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/hardware/cpp/hal/hal_dtl.c:2973
#2  0x800207f0 in _GeneralException () at
/auto/edatools/tensilica/RB-2008.4-linux/cpp/xtensa-elf/src/handlers/exc-prehandler.S:
340
#3  0x8002bc2a in cpp_reuse_req_q_insert () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/hardware/cpp/hal/hal_dtl.c:971
#4  0x802250f4 in cpp_reuse () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/cpp_reuse.c:324
#5  0x801dc3fa in chunk_free () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/chunk.c:1514
#6  0x8004d000 in ipv4_nat_free_all_seq_delta_nl () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_alg_
api.c:1219
#7  0x8004d0e1 in ipv4_nat_remove_appl_data () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_alg_
api.c:1385
#8  0x801b7eb1 in ipv4_nat_destroy_session () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_db.c
:832
#9  0x801ab07c in ipv4_nat_unlock_session () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_db.c
:1301
#10 0x801a66cc in ipv4_nat_sess_timeout () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_db.c
:1560
#11 0x801a6ce5 in ipv4_nat_sess_age () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_db.c
:1890
#12 0x801a6de0 in ipv4_nat_sess_age_to () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_time
.c:189
#13 0x80252ee4 in time_process_timer_ev () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/time.c:717
#14 0x802555e4 in process_recycle_control () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/control_rx.c:95
#15 0x80257c1e in mpass_restart_processing () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/multipass.c:1233
#16 0x820128dd in main () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/packet.c:282
```

  This symptom occurs rarely but it is more likely to occur with long-lived TCP connections.

  Workaround: A possible workaround is to lower the **ip nat trans tcp-timeout** <***n***>'value.

- CSCte84990

  In a deployment with IPsec SVTI to MPLS, down stream traffic from MPLS core is not label switching. However this might be just a broken counter because there is no traffic drop.

This symptom is observed on ASR 1000 Router Series when the "sh mpls forwarding" command is run. The Bytes Label Switched counter displays 0.

Workaround: There is no workaround.

- CSCte91369

  The following show commands will give a command line error:

  sh ip cache [prefix mask] verbose flow

  sh ip cache [prefix mask] verbose flow aggregation [aggregation name]

  This symptom is observed after the following steps:

  1. Enable netflow on ASR1000 Router using the command **ip flow ingress|egress** on any interface.
  2. Send traffic through this interface.
  3. Execute the command **show ip cache flow**. The flow entries should be displayed.
  4. Try to execute the show command to filter the flows using prefix:

     sh ip cache [prefix mask] verbose flow or

     sh ip cache [prefix mask] verbose flow aggregation [agg name]

  These commands will give a parsing error.

  Workaround: Run the same commands without **verbose** option.

  The command **show ip cache flow**, which will display all entries, will work.

- CSCte93229

  An ESP crash is observed.

  This symptom is observed on an ASR 1000 Router Series with a fragmented datagram whose size exceeds 9k and DF is set.

  Workaround: There is no workaround.

- CSCte94156

  ASR 1000 running Release 2.5.1 fails to update the PST value in TBAR, causing other GM to fail sending traffic via the ASR with anti-replay error messages. This happens wherever the local ACL is changed on the GM or by KS failure and recovery.

  This symptom is observed on ASR 1000 Router Series running Release 2.5.1 with GETVPN set up.

  Workaround: There is no workaround.

- CSCte97814

  On an ASR 1000 Router with BGP enabled, a small fixed size chunk memory leak is observed during boot-up. To be exact, it is observed just after config bulk-sync in redundant RP setup.

  This symptom is observed on Cisco ASR 1000 Series Routers with a redundant RP setup and BGP enabled.

  Workaround: There is no workaround.

- CSCtf01618

  A Cisco ASR 1000 router may unexpectedly reload due to SegV error.

  This symptom is observed on Cisco ASR 1000 routers running 12.2(33)XND1 or later XND or later 12.2(33)XN and running DMVPN with tunnel protection.

  Workaround: Move to unaffected release or remove tunnel protection.

- CSCtf06845

Cisco ASR 1000 Router crashes when receiving a crafted SNAP header.

This symptom is observed on ASR 1000 Router Series when a packet is receiving on a "encapsulation dot1Q" interface.

Workaround: There is no workaround.

- CSCtf12319

  ASRNAT with intrabox redundancy and PAT configuration in rare cases may retain session on the active much longer than what is configured (up to 4.5 hours).

  This symptom is observed when ASRNAT is running with intrabox redundancy and PAT configuration.

  Workaround: Set NAT timeouts to 15 seconds or less. Disable the second ESP.

- CSCtf12623

  A low memory condition can be seen on a Cisco ASR 1000 Router when NAT MIBs are queried.

  This symptom is observed on ASR 1000 Router Series when NAT MIBs are queried.

  Workaround: The workaround would be to exclude NAT MIB as following:

```
R5-mcp-4ru-2(config)#snmp-server view  test  1.3.6.1.4.1.9.10.77.1 excluded
R5-mcp-4ru-2(config)#snmp-server view test internet included
R5-mcp-4ru-2(config)#snmp-server community pub view test RO
```

- CSCtf15848

  The following error is seen on re-configuring channel-groups after switchover:

  EFC ERROR: spa_efc_config_ds1_channel - channel in use

  This symptom is observed with the following steps:

  1. The active RP is booted with 8xcht1/e1 and channel-group is configured on t1 controller
  2. Load the standby RP, and do a switchover
  3. On new active RP, unconfigure and reconfigure the channel-group

  Tracebacks with **EFC ERROR: spa_efc_config_ds1_channel -channel** in use are seen.

  Workaround: Before switchover, configure channel-groups on active RP when standby RP is up.

- CSCtf16359

  ASR 1000 Series Router configured as GETVPN GM will not make any local GM ACL change of removing extended ACL effective, until a new rekey from Key server.

  This symptom is observed on ASR 1000 Router Series configured as GETVPN GM.

  Workaround: There is no workaround.

- CSCtf19748

  FP crash seen on the BR with IOS XE 2.6 image. The crash happens when the MC is loaded with scaled configuration and http/ftp traffic is running.

  This symptom is observed under the following conditions:

  1. Load basic config on the MC (single prefix list, single active probe and single traffic application class).
  2. Send traffic matching the application traffic class.
  3. Load scaled configuration(ex 500 traffic classes)

  Workaround: There is no workaround.

- CSCtf22256

  FP reloads on ASR 1000 Router Series.

  This symptom is observed on ASR 1000 Router Series when using **show platform hardware qfp active feature wccp service id <*service id*>** after service is not configured.

  Workaround: Do not used show command **show platform hardware qfp active feature wccp service id <*service id*>** before valid WCCP configuration.

- CSCtf27981

  ASRNAT static network does not work properly or traceback may be received on configuration on unconfiguration.

  This symptom is only observed if 2 static networks are configured exactly the same except for network mask.

  For example:

```
ip nat inside source static network 10.1.0.0 10.2.0.0 /24 vrf vrfA
ip nat inside source static network 10.1.0.0 10.2.0.0 /16 vrf vrfA
```

  Workaround: Do not configure 2 static networks exactly the same except for network mask. If you do, it is recommended that you do the following:

  1. Remove both static network configuration
  2. Add back the 1 static network which is truly desirable.
  3. That should work, but if it does not reload the box.

- CSCtf30416

  When calling endpoint does not support T.38, the fallback is not working.

  Workaround: There is no workaround

- CSCtf32693

  On a Cisco ASR 1000 Router Series, configuring xconnect on a VLAN, SNMP 64 bit counters are not getting updated.

  This symptom is observed on a VLAN with xconnect configuration on same port.

  Workaround: There is no workaround.

- CSCtf33956

  Fragmented UDP or TCP DNS response processed by NAT ALG will be dropped.

  This symptom is observed when a DNS response is going through an ASR 1000 Series static NAT router running release 12.2(33)XND2.

  Workaround: There is no workaround.

- CSCtf40199

  A DNS response going through NAT ALG will not have the payload TTL changed 0 for same pre/post static config.

  This symptom is observed when a DNS response is going through an ASR 1000 Router Series static NAT router running release 12.2(33)XND2.

  Workaround: There is no workaround.

- CSCtf40592

  Higher latency for priority packets is observed.

For ethernet, when configuring model F broadband configuration using ANCP to change the shape rates on individual VLANs, higher latency for priority packets may be encountered. The same issue may be encountered if you remove the shaper policy-map from the VLAN and then re-apply it.

For ATM, when using multiple ATM VCs per physical interface, sustained oversubscription of that same physical interface may result in higher latency for some priority packets.

Workaround: Ethernet: Do not change the shape rate on a VLAN.

ATM: Avoid oversubscribing the interface for a sustained period of time."

- CSCtf40702

  A Cisco ASR 1000 Router Series with Route Processor 2 engine may unexpectedly reload due to a SegV crash.

  This symptom is observed if there is a monitor session configured that uses a source interface with a range. This can either be a crash while configuring via CLI or a crash at bootup if the command is in the startup config.

  Workaround: Do not use the source inter range.

- CSCtf43345

  Active and Standby FP resets on Cisco ASR 1000 Router.

  This symptom is observed during longevity run with LDAP, DNS traffic and continuous SNMP MIB Walk.

  Workaround: There is no workaround.

- CSCtf48067

  Memory leakages occur after configuring and de-configuring various netflow configurations. This includes any interface type on which netflow is configured: physical, VLANs, VT sessions, and so on.

  This symptom is observed after the following steps:

  1. Configure/De-configure netflow on physical interface.
  2. Configure/De-configure various caches.3.Configure/De-configure sub-interface(s) which has netflow enabled on it.
  3. Exporter configuration change on main and aggregation cache.
  4. Configure/De-configure virtual-interface(s) created using virtual template which has netflow enabled on it.
  5. Configure/De-configure various samplers.

  Above condition independently also leads to memory leakage.

  Workaround: There is no workaround.

- CSCtf51450

  During regular operations, the following log message was observed:

  ```
  IOSXE-6-PLATFORM: F0: cpp_cp: QFP:00 Thread:032 TS:00005645124008456668
  %LOGGER-6-DROPPED: 1 messages
  ```

  The intensity of this message was very high causing buffer and syslogs to be filled up with unwanted messages.

  This symptom is observed on ASR 1000 Router Series, running with 12.2(33)XND Release.

  Workaround: Consider filtering messages. Make use of ESM to drop these messages selectively from any of the targets (buffer, Vty/Console OR the syslog server).

- CSCtf61700

  Memory leak seen with the Radius process.

  This symptom is observed when a Radius Server (ACS) sends Access-Reject for a service profile download.

  Workaround: Make sure the service profile to be downloaded is configured in the ACS (Radius server).

- CSCtf65536

  ESP can crash while performing SIP calls using Cube-SP function.

  This symptom is observed when hairpinned SIP calls are present, but it is timing related, so it doesn't occur in all cases.

  Workaround: There is no workaround.

- CSCtf70851

  Input/Output Rate freezes and doesn't get updated.

  This symptom is observed if the interface is **shut** with the traffic running, the input/output rate gets stuck and doesn't go back to 0.

  Workaround: Giving **no shut** on the interface restarts the input/output rate.

- CSCtf85841

  The memory usage shown in the following commands keeps increasing as we repeatedly activate FRR and de-activate it by shutting and un-shutting relevant interfaces:

  sh platform software memory forwarding-manager f0 brief | inc CPP CEF MPLS MPLS

  sh platform software memory forwarding-manager f0 brief | inc frr

  This symptom is only observed if FMAN-RP receives the FRR delete request before receiving the delete request of all its child objects (out-of-order events).

  Workaround: There is no workaround.

- CSCtf86998

  In a GETVPN ASR 1000 Router Series deployment, packets on one of the ASR GM router interfaces are not encrypted.

  This symptom is observed when GM1 is in passive mode.

  Workaround: There is no workaround.

- CSCtf98758

  Standby RP crashes after replacing the basic configuration of the router with an au3-e3 configuration.

  This symptom is observed after intiating the following steps:

  1. Configure the router with back-to-back SDH link for full AU3-E3 configurations with SPA-1XCHOC12/DS0.
  2. Save the running configuration using **copy run bootflash:au3-e3.conf**
  3. Reload the router with config register set to 0x2142. This will get the router running configuration to the basic default configuration.
  4. After the router is up with redundancy setup and basic default configuration, execute the config replace command with the target config that was saved in step 1. {Config replace bootflash:au3-e3.con}

Workaround: There is no workaround.

- CSCtf98802

  Config replace command when executed in a particular way causes the router to malfunction.

  This symptom is observed after the following steps:

  1. When we try to remove channelized configuration using config replace command, it will ask for the confirmation of the same as below:

  Unprovision clear channel interface ?[confirm]

  2. If we put any character other than 'y' or 'n' it will not remove the channel configuration for that particular path.
  3. Now, if I try to remove these channels that were not cleared before manually, the system is behaves improperly:

```
Router(config-controller)#au-3 1
%ERROR: Standby doesn't support this command                            ^
% Invalid input detected at '^' marker.

Router(config-controller)#
As you see above system is not allowing to enter into the controller configuration
mode and resulting into "%ERROR: Standby doesn't support this command" message.
```

  Workaround: By this point of time only after reload of the router, the situation comes under control and then only we can alter the controller configurations.

- CSCtg00292

  Some translations getting stuck in standby router and with a **show ip nat trans verbose** we can see they have use_count as zero. This symptom is observed in a B2B NAT scenario and can happen while scaling.

  Workaround: Resetting the FP is the only workaround.

- SCtg06681

  SIP method profile allows defining a mapping of status-codes. RP2 CUBE(SP Edition) would crash while removing status-code map.

  This symptom is observed in the following configuration:

  For RP2 CUBE(SP Edition), consider the following config:

```
config t
sbc test
 sbe
  sip method-profile SIPmessage
    method INVITE
     action as-profile
     map-status-code
      range 183 value 180     <==== incorrect mapping
end
```

Note That there is only one entry for mapping status-code.

  When we try to unconfigure "range 183 value 180" as follows

  the RP2 CUBE(SP Edition) would crash:

```
config t
sbc test
 sbe
```

```
  sip method-profile SIPmessage
    method INVITE
     map-status-code
     no range 183 value 180  <=== causes crash
end
```

Workaround: The workaround is to unconfigure "map-status-code" and then re-configure it with correct mapping of status-code as follows:

```
config t
sbc test
 sbe
  sip method-profile SIPmessage
    method INVITE
    no map-status-code      <==== unconfigure map-status-code

    map-status-code         <==== re-configure
      range 180 value 183   <==== correct mapping
end
```

- CSCtg08753

  When using ASRNAT HA, if sessions on active are under SYN, RST or FIN timeout value and a switchover occurs, timeout value for those sessions goes back to TCP timeout on the new active instead of properly honoring SYN, RST, FIN timer.

  Workaround: There is no workaround.

- CSCtg23281

  At times with IP header compression enabled, the RTP timestamp is not restored to its correct value after compressing/decompressing the IP/UDP/RTP headers. This can cause jitter or one way audio. The issue occurs when an ASR 1000 Series Router is the compressor and a Cisco 2800 ISR is the decompressor.

  This symptom is observed when IP Header Compression is enabled in either Cisco original or IPHC format between an ASR 1000 Router Series and a Cisco 2800 ISR.

  Workaround: Use IETF IP Header Compression instead of Cisco original or IPHC format.

  ip rtp header-compression ietf-format periodic-refresh

- CSCtg30921

  ASRNAT pool shows allocated count of 1 when there are no addresses allocated. This means the pool can not be removed even though there are no translations off the pool.

  There is a very small timing window where this symptom occurs only for pool overload configuration. This window can happen when **clear ip nat trans *** is issued as translations are aging out. It is more likely to be seen if there are a very large number of overloaded pools.

  Workaround: The box or ESP must be reset to recover from this situation. "

- CSCtg45583

  MLP QFP client leaks memory.

  This symptom is observed if a QOS service-policy with many (7+) class-maps is configured on a Multilink interface.

  Workaround: There is no workaround.

- CSCtg52972

Configuring **ip flow-export template options sampler** on an ASR 1000 Router may stop Netflow from working and this may cause errors. It is not supported, so the command should be rejected at the CLI.

This symptom is observed when configuring the unsupported feature **ip flow-export template options sampler** on an ASR 1000 Router.

Workaround: Reload.

- CSCtg81294

  When trying to remove ASRNAT dynamic pool, the following message is observed even when there are no translations:

  %Pool <pool-name> in use, cannot destroy

  This symptom occurs in rare conditions of aging when the command **clear ip nat trans *** is run.

  Workaround: Unfortunately the only work around is to reload the box. This problem has been fixed and is only expected to be seen in B2B EFT image which just missed the fix.

Open Caveats—Cisco IOS XE Release 2.4.3

This section documents possible unexpected behavior by Cisco IOS XE Release 2.4.3.

- CSCsz01980

  The RP1 may experience unexpected watchdog timeout and reload.

  Under very rare conditions, an RP1 may experience a watchdog timeout during boot or shutdown and subsequently generate a kernel core dump.

  Workaround: No known workaround; following reload, the RP works as expected.

- CSCta24676

  On the ASR 1000 Router when an attempt is made to login to the kerberos client, the RP crashes. This is after the clocks of the UUTs are synchronized and the routers are configured with kerberos credentials.

  Workaround: There is no known workaround.

- CSCta27191

  On the ASR 1000 Router when used “upgrade rom-monitor filename harddisk:asr1000-rommon.XND.pkg all” for upgrading ROMMON the rommon failed to upgrade RP1 board on 6RU (RP2) chassis.

  Workaround: There is no known workaround.

- CSCta37670

  The ASR 1000 Router crash as a longer interrupt hold, when a single MPLS scales up to 300K prefixes. This issue occurs only when a single MPLS with 300K prefixes. The issue does not occur with 100 prefixes.

  Workaround: Not to run 300 prefixes

- CSCta76460

  On the ASR 1000 Router IPSEC EZVPN tunnels may get lost (not rekeyed properly) after a few rekey intervals.

  Workaround: Increase the rekey interval to maximum to avoid the frequency of rekeying.

- CSCtc38036

The file table overflow error will occur when the file system is being accessed.

This will occur after a few days on the ASR 1000 Router Series when running 2.4.1 and 2.4.2:

router#more system:running-config

%Error opening system:running-config (File table overflow)

Workaround: Reloading the router solves the problem, but it appears again after a few days.

- CSCtc75736

  When EIGRP is configured on the ASR 1000 Router Series the MVPN Hub role stops sending acknowledgements for reliable packets. This condition on occurs when GRE Multipoint Tunnel **shut/no shut** has been applied.

  Workaround: None

- CSCte19727

  Some IPv6 Bi-directional entries will not forward traffic on a Cisco ASR 1000 Router.

  This instance can occur when IPV6 PIM-SM and IPv6 PIM-Bi-directional are both configured on the router.

  Workaround: None

- CSCte50721

  During stateful NAT sync of H323 information from primary to standby, the standby crashes.

  This condition occurs when Cisco ASR 1000 Router with dual RP and ESP configured.

  Workaround: Is to disable H323 with the following commands when H323 ALG is not required:

  no ip nat service h225

  no ip nat service ras

- CSCte56627

  Outside NAT sessions are not syncing between active and standby.

  The following symptom may occur:

  1. Sessions may not be sync properly to standby OR
  2. session deletes may not be sync properly to standby (session that would be deleted on standby, will not be deleted).

  The following conditons may occur:

  1. On ASRNAT when there is an inside mapping and outside static mapping configuration.
  2. When there is a very high burst of session aging occurs.

  Workaround: None

- CSCte60069

  During the scale testing with ModelF applied on PTA, reparenting operation results in FP crash. Also CPUHOG and TIMEHOG tracebacks observed. The following conditions have been seen:

  1. On PTA, bring up 24K IPv4 sessions, 2PQ+2CQ (modelf)
  2. remove grandparent shaper and3)add the shaper back. When this instance occurs, FP crashes a tracebacks are observed.

  Workaround: Without the fix for this ddts, avoiding reparenting with large number of vlans with sessions will resolve the issue.

- CSCte77136

CLNS routing over GRE tunnels is not working on the ASR 1000 Router Series. When CLNS routing over GRE tunnels is configured, specifically with a GRE tunnel as the egress interface (output from the ASR 1000 Router). The CLNS packets are not forwarded via fast switching.

Workaround: Use the following configuration change on a per interface basis: **no clns route-cache** disables the clns fast switching.

- CSCte89787

  A Cisco ASR 1000 Router crashes after the Segment Switch manager reports that an invalid segment has been detected. The following logs appear on the console:

  %SW_MGR-3-INVALID_SEGMENT: Segment Switch Manager Error - Invalid segment - no segment class.

  The router will crash followed by this message.

  This has been observed on an ASR1002 running 12.2(33)XND1.

  Workaround: None known so far.

- CSCte91533

  A Cisco ASR 1000 Router is dropping small fragmented udp packet and udp fragments less than 28 bytes.

  This occurs when Windows XP Client login process to an Active Directory server in DC is slow. After the Windows client is connected to a branch site and running GETVPN across an MPLS cloud. The Cisco ASR 1000 Router is acting as a GETVPN GM Headend router.

  Workaround: None

- CSCte97907

  A Cisco ASR 1000 Router with RP2 gets out of sync with NTP master every 18 minutes for approximately 1 minute. The offset to the NTP master increases up to -1052.1 msec and the sync gets lost.

  This occurs when NTP is **enabled** and running aproximately 20 minutes.

  Workaround: None

- CSCtf01618

  A Cisco ASR 1000 Router may unexpectedly reload due to SegV error.

  This condition has been observed, when the ASR 1000 Router must be running 12.2(33)XND1 or later XND or 12.2(33)XNE or even later 12.2(33)XN releases and DMVPN is configured with Tunnel Protection.

  Workaround: 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. When destination of VC is changed from original to something else and then changed back to original.

  Workaround: None.

Resolved Caveats—Cisco IOS XE Release 2.4.3

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.4.3

- CSCse97209

  On a Cisco ASR 1000 Router Series standard communities are not set correctly by an outbound route-map.

  This occurs when ***route-map uses*** continue option is used.

  Workaround: There is no workaround.

- CSCsk85192

  On a Cisco ASR 1000 Router copy command arguments followed by a ":" are not sent to ACS when command authorization is enabled. This includes scp:, ftp:, tftp:, flash:, etc. On enabling parser ambiguity debugs its seen that the arguments with colon are not matched with the existing keywords though its a valid directory.

  Workaround: Is to deny or permit the full copy command for users.

  Further Problem Description: This issue affects AAA Authorization. When the argument is specifically denied by ACS that arguement will be able to be run on the IOS device. If the arguement is specifically allowed by ACS with default arguements being denied the commany followed by a ":" will not be able to be run.

- CSCso18626

  Destinations via MLPPP sessions may become unreachable following a RP switchover. When MLPPP sessions are active, BGP nexthops are reachable via the MLPPP session prior to a switchover. An RP switchover then occurs.

  Workaround: The affected multilink interfaces can be shut/no shut i.e.

  shut/no shut interface multilink

  Repopulating the routes in the affected VRF(s)will also restore reachability.

  clear ip route vrf FOO

- CSCso18626

  Destinations via MLPPP sessions may become unreachable following a RP switchover. When MLPPP sessions are active, BGP nexthops are reachable via the MLPPP session prior to a switchover. An RP switchover then occurs.

  Workaround: The affected multilink interfaces can be shut/no shut i.e.

  shut/no shut interface multilink

  Repopulating the routes in the affected VRF(s)will also restore reachability.

  clear ip route vrf FOO

- CSCso60442

  A crash occurs on a Cisco ASR 1000 Router Series.

  This symptom is observed when the **show buffers interface dump**command is entered.

  Workaround: There is no workaround.

- CSCsv36976

  After the display of the 1000 characters on the console, if there are more to display, the display is truncated. The problem happens when you have large number of interfaces and the output of "show zone security" is larger than 1000 characters.

Workaround: The workaround is to show all interfaces and get the zone membership from the interface.

Further Problem Description: The root cause of the problem is that the display buffer for this command is limited with 1000 characters."

- CSCsv36976

  A Cisco ASR 1000 Router running IPSec (IP Security) can run at high cpu up to 100% indefinitely in the “Crypto IKMP” process.

  This problem can occur when there is error conditions internal to the IKE process.

  Workaround: The workaround is to issue the command **clear crypto isakmp** to clear theIKE SA's.

- CSCsx10028

  A core dump may fail to write or write very slowly (less than 10KB per second) on the Cisco ASR 1000 Router Series.

  The symptom is observed when the cause of the crash is processor memory corruption. When this occurs, the corrupted memory pool cannot be used to write the core dump so it will likely fail. (IO memory corruption crashes should not have this problem.)

  Workaround: There is no workaround.

  Further Problem Description: This bug also increases the default size for the exception memory region to 256K to make sure it has enough memory to handle writing core dumps. This means that it is no longer necessary to adjust it as per the core dump instructions on CCO.

- CSCsx15841

  The **BGP aggregate-address** command configured on active RP does not auto-sync to the running configuration of the standby RP.

  This occurs when BGP is configured on active and standby redundant RP system(s).

  Workaround: Configure BGP aggregate-address and reboot the system, forcing both active and standby to load from startup configuration.

- CSCsx30395

  When all interfaces are **shut**, wait 5 secs, and then **no shut**, then LDP session is not reestablished for one link peer. This seen only on ASR 1006 with VPNs on GigE dot1q interfaces, some with AToMPLS.

  Workaround: Clear sessions with **clear mpls ldp nei ***.

- CSCsx83443

  ISKMP debug messages from all peers are shown in the terminal monitor enable tty/vty's even though **debug crypto condition peer ipv4 x.x.x.x** is set.

  This condition can occur when using peer IP-based debug condition.

  Workaround: There is no workaround.

  Further Problem Description: Only a subset of the messages are shown.

- CSCsy10893

  A Cisco ASR 1000 Router reloads occasionally after the command **show buffers leak** is repeatedly issued.

  The symptom is observed when issuing the **show buffers leak** command. This occurs only with certain patterns and scale of traffic and does not occur all the time.

Workaround: There is no workaround.

- CSCsy45371

  The **clear ip nat tr *** command removes corresponding static NAT entries from the running configuration, but removing static NAT running configuration does not remove the corresponding NAT cache.

  This may occur, when NAT commands are entered while router is processing around 1 Mb/s NAT traffic.

  Workaround: Is to stop the network traffic while configuring NAT.

- 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: None

- CSCsz15295

  The GM failed to register when fail-close feature is enabled with missing ACL.

  This instance has occurred when configuring fail-close that gives a matching ACL and activates. In addition, do not configure ACL in global configuration.

  Workaround: Is to deactivate fail-close.

  Further Problem Description: GM failed to register when fail-close feature is configured with a non-existing ACL.

- CSCsz56462

  When configuring cdp run it does not bring up cdp on the interfaces. This Conditions happens only if the default behaviour of a platform is to have CDP disabled.

  Workaround: To enable CDP, include the cdp enable command in the configuration.

- CSCsz72591

  On a Cisco ASR 1000 Router crashes with an Address Error (load or instruction fetch) exception. The router must be configured to act as a DHCP client.

  Workaround: There is no workaround.

- CSCsz74859

  NHRP cache entry is not getting created for certain spoke nodes on a Cisco ASR 1000 Router Series.

  This symptom occurs when two spokes A and B advertise the same subnet with varying masks (anything other than /8 or /16 or /24). A third spoke upon receiving such routes (from the hub), in order to send traffic to such subnets, can form a dynamic tunnel with either A or B but not both at the same time.

  Workaround: There is no workaround.

  Further problem description: There is no hindrance to traffic since it continues to flow via the hub. When tunnel with spoke A is formed, there is no problem with traffic to subnet behind spoke A. But, traffic to subnet behind spoke B takes the spoke A - hub - spokeB path. This can be easily noted by traceroute.

- CSCta26029

  Path attribute memory leak is found when there is some path attribute churn in the network.

  The symptom is seen only when there are idle peers on the router.

Workaround: Unconfigure the idle peers.

- CSCta38072

  Cisco IOS XE may fail while attempting to do a "redundancy force-switchover." This is an intermittent issue.

  During a "redundancy force switchover," the switchover occurs, but when standby bay 0 is restarting, Cisco IOS XE fails. Cisco IOS XE in standby bay 0 then restarts and the system reaches SSO.

  Workaround: There are no known workarounds.

- CSCta48816

  On a Cisco ASR 1000 Router running ODR as a routing protocol for a DMVPN deployment, might display similar message:

  Jun 9 03:40:44.141: %SYS-2-GETBUF: Bad getbuffer, bytes= 32717 -Process= "CDP Protocol", ipl= 2, pid= 157

  These messages have been seen on Cisco ASR 1000 Router running software 12.2(33)XNC1.

  Workaround: Use a routing protocol which does not rely on CDP in the DMVPN cloud (passive RIP, RIP, BGP or EIGRP).

- CSCta93640

  Next-hop tracking notification is sent even though track is undefined. This has been observed, when PBR is configured with the set next-hop tracking.

  Workaround: None

- CSCtb13421

  The GM may not register on a Cisco ASR 1000 Router Series. This symptom has been observed, when a crypto map with local-address is configured and applied on multiple interfaces, after one of these interfaces are then shut.

  Workaround: Is to disable local-address for the crypto map.

- CSCtb32502

  With a 1K DMVPN spoke, unconfigure/ re-configure tunnel protection several times and unconfigure/re-configure a tunnel interface, the RP resets.

  Workaround: Wait until all DMVPN session is up or down before next unconfig/re-config tunnel. That is, do not unconfig/re-configure tunnel when there are many sessions in transaction state.

- CSCtb67461

  When pado delay per circuit id is configured for different strings in the PTA device, the circuit id needs to be matched with each entry in the list until a match is found. But this does not happen. Only the first string is tried to be matched and if a match not found, no pado delay is applied. This is the same case for remote id.

  Workaround: None

- CSCtb74547

  On a Cisco ASR 1000 Router Series DMVPN HUB reloads when processing IPSEC key engine.

  This conditions happens when dual DMVPN with shared tunnel protection feature is enabled.

  Workaround: None

- CSCtb89424

In rare instances, a Cisco ASR 1000 Router may crash while using IP SLA UDP Probes configured using SNMP and display an error message similar to the following:

hh:mm:ss Date: Address Error (load or instruction fetch) exception, CPU

signal 10, PC = 0x424ECCE4

This symptom is observed while using IP SLA on the router.

Workaround: There is no workaround.

- CSCtb89767

  A problem may occur on an FP20 when configuring the IPSEC part of the SVTI topology the delete and reconfig of IPsec does not happen. This has been seen in a FP20 SVTI IPSEC setup with 1 tunnel configured.

  Workaround: Is to reload the router.

- CSCtc21042

  A chassis-manager processed on RP2 gets stuck and the router becomes unresponsive to user commands. All the FPs and CCs keep rebooting, with console logs showing repeated FP code downloads.

  This problem is specific to RP2. No particular scenario is known. Problem is caused by OBFL logging of messages on RP2.

  Workaround: Is to disable onboard logging of messages on RPs as follows:

  “hw-module slot r0/r1 logging onbaord disable”

  Router#hw-module slot r0 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.

- CSCtc25464

  After the ASR 1000 Router Series has been reloaded, and the tunnel interface has been configured with keepalives it will remain in the line-protocol down state. This will occur only when keepalives are configured for a short interval (total timeout under 10 seconds) and when the box has been reloaded.

  Workaround: Is to remove the keepalive configuration on the tunnel and to reload the configuration again; after the router has rebooted when the tunnel interface is still down.

- CSCtc30420

  CPP tracebacks are logged after configuring the ASR 1000 Router Series as an RP2 with IPSec DMVPN Spoke. Only in this condition, when unconfiguring DMVPN on the router and reconfiguring it again, CPP tracebacks are logged.

  Workaround: Is to reload the router.

- CSCtc38484

  The giga word counters are not reflecting properly in the stop record.

  When the interim accounting is enabled, the giga-word counters are reflecting fine in interim and stop record. This occurs on the ASR 1000 Router.

Workaround: There is no issues when the interim record is enabled. When the interim accounting is disabled on the ASR 1000 Router, execute the show interface virtual command. This will allow for the giga word counter in the stop record to be confiigured.

- CSCtc40677

  The distribute-list applied to the virtual-template interface is not effective for the virtual-access interfaces spawned by that template.

  For example, configured on the ASR (hub) is:

```
router eigrp 1
 redistribute static metric 10000 100 255 1 1500
 network 10.0.0.0
 no auto-summary
 distribute-list prefix TEST out Virtual-Template1!
ip route 0.0.0.0 0.0.0.0 Null0
ip route 10.0.0.0 255.0.0.0 Null0!
ip prefix-list TEST seq 10 permit 0.0.0.0/0
ip prefix-list TEST seq 20 permit 10.0.0.0/8
```

  For example: On the branch site when connected to a Virtual-accessinterface will show as:

```
ranch#sh ip route eigrp
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, *15:56:44.397 BRU Wed Oct 7 2009
10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D       10.0.0.0/8 [90/46251776] via 10.12.0.2, 00:00:06, Dialer1
D       10.1.1.0/24 [90/46228736] via 10.12.0.2, 00:00:06,Dialer1
D       10.2.2.0/24 [90/46354176] via 10.12.0.2, 00:00:06, Dialer1
D*EX 0.0.0.0/0 [170/46251776] via 10.12.0.2, 00:00:06, Dialer1
```

  This shows that no filtering was applied, since the 10.1.1.0/24 and 10.2.2.0/24 should have been dropped off the updates.

  The symptom is observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 12.2(33)XND1.

  Workaround: Configure the distribute-list for the specific virtual-access interface used for the connections on the hub.

- CSCtc43110

  Under H.323 call scenarios, outgoing H.323 signaling packets (TCP) are marked with a non-zero DSCP value, even though no QoS is configured for H.323 calls. This happens under all H.323->H.323 and SIP->H.323 scenarios when SBC creates a downstream H.323 calls.

  Workaround: There is no workaround with SBC configuration. QoS can be re-marked when MQC policy is placed on the outbound physical interfaces of the ASR 1000 Series Router.

  Workaround: None

- CSCtc45681

  QoS Accounting stats is incorrect after changing the policer rate.

  The following conditions have been observed:

  1. ASR1004 is configured as PTA.
  2. QoS Accounting is enabled at the output policy-map voip class.
  3. Pass traffic for 10 seconds.
  4. Stop traffic and verify the interim-update record has the correct QoS accounting stats.
  5. Re-start traffic.

6. Under traffic load, modify the voip class police rate.
7. Verify the voip traffic is now policed to the new rate.
8. Stop traffic.
9. Run show cmd: show policy-map session output.

Note Note the voip class conformed pkt/byte counts.

10. Check the accounting interim record. Notice that the pkt/byte counts do not match those form the show cmd output in step 9.

Workaround: Remove and reapply the QoS policy-map.

- CSCtc51048

  On the Cisco ASR 1000 Router the FP will reset, when configuring "**show platform hardware cpp feature ipsec spd all**" on the cli, after deleting tunnels FP crash on "**sh pla hard cpp feature ipsec spd all"** while deleting tunnels. This condition will occur when tunnel has been deleted and applyed to the CLI "**show platform hardware cpp feature ipsec spd all**" both even should happen together.

  Workaround: Do not apply CLI "**show platform hardware cpp feature ipsec spd all**" while you are deleting number of tunnels.

- CSCtc53381

  Encryption with decryption fails after deleting and creating a IPSecv6 Tunnel on a Cisco ASR 1000 Router.

  This problem is seen after deleting and recreating a IPSecv6 Tunnel.

  Workaround: None

- CSCtc65800

  FP reloads when crypto map is removed from interface in CAC-ACL configuration on a Cisco ASR 1000 Router.

  This occurs only when CAC ACL configuration is used. Plain ACL with match address will not have any FP reload issue.

  Workaround: None

- CSCtc65800

  A virtual reassembly error message of the FRAG-REASSEMBLY_DBG type is seen and the traceback decode of the error message points to the ipv4 vfr refrag function indicating packet drop. The issue may cause another ATTN_NOTIFY timeout error message in about 4 minutes.

  The condition was observed under uRPF drop on broadband LNS virtual interface. In general other virtual reassembly drops at ipv4 vfr refrag due to malform fragments may trigger the issue.

  Workaround: Un-configure vitrual reassembly or avoid the specific packet drop condition.

- CSCtc68037

  A Cisco IOS XE device may experience an unexpected reload as a result of mtrace packet processing.

  Workaround: None other than avoiding the use of mtrace functionality.

- CSCtc86951

On the ASR 1000 Router Series, when high speed logging is enabled for NAT, ESP may fail after a RP SSO switchover. In rare conditions when high speed logging is enabled for NAT, ESP may fail after a RP SSO switchover.

Workaround: None

- CSCtc87822

  On a PE router, eBGP-learned VRF routes might not be advertised to eBGP neighbors in the same VRF.

  The symptom is observed if DUT first learns the route from IBGP-VPNv4 (same RD) and then learns the route from the CE.

  Workaround: Soft clear towards the CEs missing the routes.

- CSCtc95423

  Router crashes when quickly unconfiguring and reconfiguring crypto maps on a Cisco ASR 1000 Router.

  This may only occur, when crypto is turned on while SAs are still being deleted in the background and duplicate SAs may be created, which may cause the router to crash.

  Workaround: Before re-applying crypto maps, wait until all SAs on the router are deleted before turning crypto back on.

- CSCtc96161

  DMVPN is working fine for a ~week and then one of spokes appears to be no longer able to pass traffic to other spokes. IPSEC tunnel between the spokes can be established at IOS level, but cannot be programmed into hardware and traffic is not getting through.

  This problem is only seen when there are more spoke to spoke dynamic tunnels and the dynamic tunnels are flapping frequently for a long period of time.

  Workaround: Reduce the frequency of dynamic tunnel flapping by increasing NHRP hold down timer to avoid tearing down dynamic tunnels too often. This can reduce the chance of hitting the problem. But when the problem happens, the affected spoke has to be reloaded.

- CSCtd00493

  For IPv6 Bi-directional entry FF03::1:0:0/96, some packet with address like FF03::1:1:1/128 or FF03::1:1:2/128, etc… In addition a Cisco ASR 1000 Router cannot find a match in CPP due to the collision lookup failure. This problem may cause the traffic to not forward the entries on the router.

  Workaround: None

- CSCtd00644

  The ASR 1000 Router Series may restart ungraceful with scaled config. When there is scaled config and sessions are flapping frequently, only on rare instances the ASR 1000 Router Series may restart ungracefully. This problem may also timing related, so it may not happen with every time sessions flaps.

  Workaround: None

- CSCtd02123

  WRED state only shows WRED state with standard class.

  In **sh policy-map int**, WRED state only show standard class's WRED state.

  Workaround: Is to only use standard wred classes.

- CSCtd02554

  The following error message may show up when AAA is used by the PPPoE:

%AAA-6-BADHDL: invalid hdl AAA ID 0, hdl CE010AA1, retired -Process= “SG CMD HANDLER”, ipl= 0, pid= 151

This could happen during the scalability test with large number of PPPoE sessions.

Workaround: None

- CSCtd15634

  Traceback seen on a Cisco ASR 1000 Router console indicating an error.

  This condition occurs when bringing up an L2-Connected ISG session and then immediately sending a non-stop Service Activation and Deactivation CoA.

  Workaround: Do not send a non-stop Service Activation and Deactivation CoA immediately after bringing up an L2-Connected ISG session.

- CSCtd17681

  Multicast hello packets are not encrypted by IPSec resulting in failure to setup OSPF with EIGRP sessions.

  This Issue has been seen in a DMVPN setup, or when a point to point Frame-Relay IPSec session is configured.

  Workaround: None

- CSCtd35091

  The input queue on ISG's access interface gets filled up causing the interface to wedge.

  The symptom is observed when an L2-connected IP session for a client exists on the ISG and traffic from that client comes in with a different IP address to the one used to identify the session. This traffic is dropped and interface wedging is observed.

  Workaround: There is no workaround other than a router reload.

- CSCtd38225

  When ISG is enabled and DHCP sessions re-start just around the time their leases expire, some sessions may get stuck dangling indefinitely. Sending DHCP DISCOVER message (i.e.: re-starting the CPE) will not restore the session. The affected subscriber(s) will not be able to establish a session.

  The issue seems to be a corner-case situation. It is observed when ISG is enabled and DHCP sessions re-start just around the time their leases expire.

  Workaround: The only known workaround is to manually clear the dangling session(s) using the **clear ip subscriber dangling <*time*>** command although this may not be a suitable workaround in a live production network.

- CSCtd39778

  The Cisco ASR 1000 Router may reset due to IOS failure, when ZBFW is configured with more than 16 match protocols and there are large an additional no match protocl statements in ZBFW class-maps.

  This has been seen, when an addition of more than 16 match protocol statements in a class-map is used for inspect policymap on the ASR 1000 Router.

  Workaround: Is to split the class-map with more than 16 match protocol into multiple class-maps, each with 16 or less match statements.

- CSCtd47550

  On an ASR 1000 Router configured with redundant RP's and a scaled ISG configuration, the ESP fowarding processor may reload during an RP switchover.

Defect requires redundant RPs and a scaled ISG configuration with many active ISG sessions. An RP switchover also seems to be a necessary condition.

Workaround: No known workaround.

- CSCtd47813

  Traffic loss may be seen after rekey between the Cisco ASR 1000 Router Series acting as GMs when modifying KS ACL. This may only occur, when a more specific permit statement has been added. In addition, when permit ip any any has been applied this will result in traffic loss when rekeying the router.

  Workaround: Is to keep permit ip any as the last acl in the KS ACL set.

- CSCtd48203

  On a Cisco ASR 1000 Router, after the last cache engine in a WCCP service group goes away, packets start getting dropped instead of being forwarded to original destination.

  This problem occurs when the last cache engine present in a WCCP service group becomes unavailable.

  Workaround: To overcome this problem, remove the global service group definition of the service group whose all CEs have become unavailable by using the following CLI conf t:

```
conf t
 no ip wccp <web-cache | service-group-id>
   (or)
Remove the redirect in config from the interfaces on which the service group is
attached, like
conf t
 int <interface name>
 no ip wccp <web-cache | service-group-id> redirect in
```

- CSCtd48500

  SNMP 64 bit counters not showing traffic. This has seen seen on ASR1002 running 12.2(33)XND1 and XND2 after deploying an AToM Circuit under it.

  Workaround: None

- CSCtd49249

  The following error message shows up during the uSBC config:

```
%Log packet overrun, PC 0x111B639, format:
%s

log:

config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#sbc test
Router(config-sbc)#sbe
Router(config-sbc-sbe)#adjacency sip sippa
Router(config-sbc-sbe-adj-sip)#no attach
Router(config-sbc-sbe-adj-sip)#account sipp-a
Router(config-sbc-sbe-adj-sip)#fast-register disable
Router(config-sbc-sbe-adj-sip)#remote-address ipv4 1.2.37.19 255.255.255.255
Router(config-sbc-sbe-adj-sip)#registration rewrite-register
Router(config-sbc-sbe-adj-sip)#signaling-address ipv4 107.1.1.1
Router(config-sbc-sbe-adj-sip)#signaling-peer 1.2.37.19
Router(config-sbc-sbe-adj-sip)#signaling-peer-port 5060
Router(config-sbc-sbe-adj-sip)#signaling-port 5088
Router(config-sbc-sbe-adj-sip)#attach

%Log packet overrun, PC 0x111B639, format:
```

```
%s
Router(config-sbc-sbe-adj-sip)#end
Router#
```

Workaround: None

CSCtd50125

GetVPN on a Cisco ASR 1000 Router GM fails to download the TEK information in the hardware [debug crypto ipsec output below] *Nov 27 02:20:38.323: IPSEC(download associate flow):

```
flow_info: in_flow_id: 2400005F, out_flow_id 24000060
    out_flow_enable: 0
    acl_line_num 1
    sadb_root_local_add: 172.16.0.1
local_proxy: , remote_proxy:
    in_spi: 35EB57B0, out_sp
*Nov 27 02:20:43.341: IPSEC(crypto_ipsec_create_transform_sas): Failed to attach
flowid to hw
*Nov 27 02:20:43.342: IPSEC(delete_sa): deleting SA,
  (sa) sa_dest= 172.16.0.1, sa_proto= 50,
    sa_spi= 0xD2A8F435(3534287925),
    sa_trans= esp-aes 256 esp-sha-hmac , sa_conn_id= 2093    sa_lifetime(k/sec)=
(0/115),
  (identity) local= 172.16.0.1, remote= 0.0.0.0,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4)
*Nov 27 02:20:43.342: IPSEC(update_current_outbound_sa): updated peer 0.0.0.0 current
outbound sa to SPI 3751CFC3
*Nov 27 02:20:43.342: IPSEC(delete_sa): deleting SA,
```

This condition has been observer, when IPv6 configured on the crypto map local address,

Workaround: Is to disable IPv6 and reload the box.

- CSCtd53112

  IOS reload occurs when on a Cisco ASR 1000 Router when ‘debug cond ip nat inside source static..’ command entered and NAT has never been configured on the box.

  Workaround: Enter 'debug cond ip nat' commands only after NAT has been configured.

- CSCtd54632

  System console may not response on the Cisco ASR 1000 Router Series.

  This symptom is observed on a Cisco ASR 1000 Router Series when functions as an IP Security (IPSec) termination and aggregration router, and when a self-signed cerificate is configured during Forwarding Processor (FP) is out of service.

  Workaround: There is no workaround. The console will be back to service when FP is active or when the request gets timeout'ed (around 480 seconds).

- CSCtd67034

  The following error message is seen on a Cisco ASR 1000 Router “%CPPHA-3-FAULT: F0: cpp_ha: CPP:0 desc:...” and accompanying crash dump of the CPP QFP complex.

  The various errors which have been seen in association with this problem include:

  “%CPPHA-3-FAULT: F0: cpp_ha: CPP:0 desc:...”

  where desc: could be any of the following errors:

  ```
  Desc: ETC_ETC_LOGIC1_LEAF_INT_INT_ETC_LKUP_DATA_ERR
  Desc: ETC_ETC_LOGIC2_LEAF_INT_INT_GPM_ENQ_VTL_DROP_ERR
  Desc: GAL_GAL_CSR_IPM_IF_GAL_IPM_IF_LEAF_INT_INT_IPM_ERR
  Desc: GRW_GPM_GRW_CSR_RDWR_UNIT_0_GPM_RW_LEAF_INT_INT_REQUEST_ERROR
  Desc: GRW_GPM_GRW_CSR_RDWR_UNIT_1_GPM_RW_LEAF_INT_INT_REQUEST_ERROR
  ```

```
Desc: GRW_GPM_GRW_CSR_RDWR_UNIT_2_GPM_RW_LEAF_INT_INT_REQUEST_ERROR
Desc: GRW_GPM_GRW_CSR_REQ_TOP_GPM_REQ_LEAF_INT_INT_MAP_ICREQ0_NO_CONTEXT
Desc: OPM_OPM_INT_REGS_OPM_META_LEAF_INT_INT_UNDEF_DESC
Desc: PQS_PQS_LOGIC1_INTR_LEAF_INT_INT_OUT_OF_RANGE_Q_ERR
Desc: SRT_SRT_PAR_ERR_LEAF_INT_INT_STEM_0
```

A corner case issue was discovered where the FRF.12 (Frame Relay Fragmentation) and MLP (Multilink PPP) features were susceptible to various hardware detected error conditions when performing fragment reassembly for cases where the last fragment was a few bytes in length (approx. 4-8 bytes of payload after the protocol headers).

This condition has only been seen with high traffic rates in conjunction with the small end fragment condition.

Workaround: None

- CSCtd70582

  Traffic Class services will remain in “show subscriber session” output under "Policy Information" after traffic class has disconnected by timer events.

  Only seen when Traffic Class is disconnected through an Idle Timer or Absolute Timer expiring.

  Workaround: When traffic class service is disconnected through normal (User Intervention), issue is not seen. For Timer disconnected Traffic Class services, no known workaround at this time.

- CSCtd79978

  A Cisco ASR 1000 Router crashes after issuing a “**show pppoe throttled subinterfaces** “command.

  This issue has been seen on ASR 1000 Routerrunning 12.2(33)XND2 IOS.

  Workaround: Not execute the show command.

- CSCtd90265

  IP Security (IPSec) functionality stops working, when Route Processor (RP) CPU rate can be high.

  This symptom is observed on a Cisco ASR 1000 Router Series when functions as an IP Security (IPSec) termination and aggregration router, after super package In-Service Software Upgrade (ISSU) was performed with IPSec traffic running.

  Workaround: There is no workaround.

- CSCte05638

  Cannot copy WebEx application logs from WebEx Node SPA console with Vegas shell commands.

  When connection to WebEx Data Center fails, the WebEx support team might need to look at the

  WebEx application log files to identify the problem.

  There is no mechanism today for customer to copy this logs files out of the WebEx Node SPA.

  Workaround: None

- CSCte19782

  When ESP traffic is traversing NAT with inside static configs, the traffic initiated from the outside hosts willl not work.

  This condition happens with NAT inside static configuration, the ESP traffic iniitated from the outside network will be passing through the NAT box untranslated.

  Workaround: There is no known workaround.

- CSCte20171

HSRP active router send ICMP redirect message that source address set to physical interface IP address. The Virtual IP address should be used as source address.

Workaround: None

- CSCte20928

  ESP20 restarts when loading the config on the RP2.

  This issue has been seen when loading config on a blank box with ESP20 and RP2.

  Workaround: None

- CSCte40621

  On a Cisco ASR 1000 Router when adding pinhole, after modify has failed with an ER=421 error message.

  For example: “AddIssue-NG.pcap” contains failed pattern with following order:

```
- ADD (pinhole ntt/user1a)
- ADD (pinhole ntt/user2a)
- Modify (pinhole ntt/user1a)
- ADD (pinhole ntt/user2v)   -> failed with ER=421
```

  Workaround: None

- CSCte45106

  Crash in QoS cpp_cp process when memory is running to slow on the Cisco ASR 1000 Router Series.

  The following conditions have been observed:

  1. Establish 25k PPPoE PTA ISG sessions with traffic classes, port bundle, l4r, accounting and QoS.
  2. Send traffic through the sessions.
  3. Make sure that all the idbs are used.
  4. Keep trying to establish PPPoE sessions.
  5. FP crash should be observed.

  Workaround: Keep memory from running low.

- CSCte45509

  The ASR 1000 Router cannot take over PPP and L2TP sessions when ISSU has been loaded .

  During ISSU step, active RP image is a previous version and Standby RP image

  is 12.2(33)XND3.

  The following traceback occur and cannot create ppp sessions on standby RP.

  %SYS-2-LINKED: Bad enqueue of xxx in queue xxx -Process= “RADIUS”

  Therefore all PPP sessions is lost at the time of RP switchover.

  Workaround: There is no workaround.

- CSCte46218

  Traffic is not forwarded through GRE or multipoint GRE tunnels with “tunnel key 0”. This condition is seen when tunnel key is configured via ""no tunnel key"" and then reconfigured via “tunnel key 0” on a GRE or mGRE tunnel, traffic will received tunnel packets will be dropped.

  Workaround: After removing tunnel key configuration, configure “tunnel key” with non-zero value or delete and recreate tunnel interface.

- CSCte89787

  An ASR 1000 Router crashes after the Segment Switch manager reports that an invalid segment has been detected.

  The following logs have been observed:

  %SW_MGR-3-INVALID_SEGMENT: Segment Switch Manager Error - Invalid segment - no segment class.

  The router will crash followed by this message.

  This has been observed on an ASR1002 running 12.2(33)XND1.

  Workaround: None

- CSCte91533

  A Cisco ASR 1000 Router may drop small fragmented udp packets, the udp fragments are less than 28 bytes. This condition has been observed when Windows XP Client login processes to an Active Directory server in the DC is slow. In additon, when Windows client is connected to a branch site and running GETVPN across an MPLS cloud. An ASR 1000 Router is acting as a GETVPN GM Headend router.

  Workaround: None

- CSCte97907

  On a Cisco ASR 1000 Router with RP2 gets out of sync with ntp master every 18 minuted for approximately 1 minute. This offsets the master and increases up to -1052.1 msec and the sync gets lost.

  This conditions may happen when NTP is enabled and running aproximately 20 minutes.

  Workaround: None.

- CSCtf14254

  Ucode crash has been seen with Multicast Nat configured on a Cisco ASR 1000 Router. This has been observed after configuring Multicast Nat on the router. This may cause a ucode crash.

  Workaround: None

- CSCtf18200

  Traffic loss during sub package ISSU for Release 2.4.3 to Release 2.6.0 after CC upgrade stage. This conditions has been seen when Gig based SPA interface with vlan is configured.

  Workaround: Traffic will resume once the RP upgrade is complete.

Open Caveats—Cisco IOS XE Release 2.4.2

This section documents possible unexpected behavior by Cisco IOS XE Release 2.4.2.

- CSCsy49927

  The IOSd restart is seen with RP2 at proc frame when using the tcl shell for execution. This is seen with crest proc that helps in configuring a scale config.

  Workaround: None

- CSCsz01980

  Under very rare conditions, the RP1 on a Cisco ASR 1000 Series Router may experience an unexpected watchdog timeout during boot or shutdown and reload.

  Workaround: None

  Following the reload, the RP1 works as expected

- CSCsz56462

  When configuring **cdp run** it does not bring up cdp on the interfaces. This Conditions happens only if the default behaviour of a platform is to have **CDP disabled**.

  Workaround: To **enable CDP**, include the cdp enable command in the configuration.

- CSCta22480

  When the **show memory debug leaks** or **show memory debug leaks chunks** command issues an output report it may not be accurate. In addition the **show memory debug leaks command** is not used under normal router operations; and this will not affect normal router behavior.

  Workaround: There is no known workaround.

- CSCta24676

  On the ASR 1000 Router when an attempt is made to login to the kerberos client, the RP crashes. This is after the clocks of the UUTs are synchronized and the routers are configured with kerberos credentials.

  Workaround: There is no known workaround.

- CSCta27191

  On the ASR 1000 Router when used "upgrade rom-monitor filename harddisk:asr1000-rommon.XND.pkg all" for upgrading ROMMON the rommon failed to upgrade RP1 board on 6RU (RP2) chassis.

  Workaround: There is no known workaround.

- CSCta37670

  The ASR 1000 Router crash as a longer interrupt hold, when a single MPLS scales up to 300K prefixes. This issue occurs only when a single MPLS with 300K prefixes. The issue does not occur with 100 prefixes.

  Workaround: Not to run 300 prefixes

- CSCta45697

  On the ASR 1000 Router high priority IPsec traffic could be dropped.

  This will occur When total throughput of high priority and low priority IPsec traffic oversubscribed the encryption/decryption engine.

  Workaround: Reduce IPsec traffic bandwidth to below threshold.

- CSCta48816

  On the ASR 1000 Router running ODR as a routing protocol for a DMVPN deployment, might display similar message:

  Jun 9 03:40:44.141: %SYS-2-GETBUF: Bad getbuffer, bytes= 32717 -Process= "CDP Protocol", ipl= 2, pid= 157

  These messages have been seen on ASR 1000 Router running software 12.2(33)XNC1.

  Workaround: Use a routing protocol which does not rely on CDP in the DMVPN cloud (passive RIP, RIP, BGP or EIGRP).

- CSCta76460

  On the ASR 1000 Router IPSEC EZVPN tunnels may get lost (not rekeyed properly) after a few rekey intervals.

  Workaround: Increase the rekey interval to maximum to avoid the frequency of rekeying.

- CSCtb07473

  On the ASR 1000 Series this is seen during router booted up after ISSU software upgrade and redundancy forceswitchover. This issue will occur when bringing up the console dump: show ipc session rx verbose, IOSd crashed at ipc_print_flow_control_statistics.

  Workaround: Use a local data structure to keep the contents of port_info.

- CSCtb07984

  he ASR 1000 Router acting as a LNS router failed to apply D2 QOS on first 2 PPPoX sessions after every new reboot and configures D2 QOS on all subsequent sessions. This occurs when PPPOX sessions are brought on LNS with D2 QOS model after new reboot of router.

  Workaround: LNS router configures D2 QOS on all subsequent sessions

- CSCtb29156

  The LNS will bring up Sessions without VRF configuration when Radius Customer template is used. The symptoms are when the PPPoX session are up and it will get the ip address from designated VRF pool.

  Workaround: Use local Customer template and vpdn configuration

- CSCtb49373

  On the ASR 1000 Router Series if there is no less than a specific static route including the prefix of the static route in the table it will stay in the routing table although both routes should be removed.The Static route pointing to next-hop (without exit interface) does NOT get removed from routing table when route towards next-hop disappears.

  Workaround: Specify an exit interface in addition of next-hop

- CSCtb51418

  On the ASR 1000 Router Series the RP will reload while flapping the sessions overnight.

  The RP will reload while running the following overnights:

  - Flap 8000 sessions once in every 20mins
  - ESIC,ISIC tools for sending invalid packets
  - RCMD script which does a rsh to the router and executes show commands continuously
  - Uploading files continuously to the router using tftp copy

  Workaround: None

- CSCtb56852

  RP resets when we delete DMVPN Tunnel on hub router .

  In 1hub and 1000 spokes scenario, when we delete dmvpn tunnel on hub causes RP reset on hub router.

  Workaround: None

- CSCtb89767

  When the FP20 svti ipsec setup with 1 tunnel has been configured the ipsec part of the svti topology will be deleted; and re-configing the IPsec does not happen.

Workaround: Reload the router.

- CSCtc02012

  When using GETVPN with authentication based on preshared keys rhe KS sends, as ID payload in Main Mode 6, protocol 17 [udp] port 500 instead of protocol 17 [udp] port 848.

  Workaround: None

- CSCtc25464

  After the ASR 1000 Router Series has been reloaded, and the tunnel interface has been configured with keepalives it will remain in the line-protocol down state. This will occur only when keepalives are configured for a short interval (total timeout under 10 seconds) and when the box has been reloaded.

  Workaround: Is to remove the keepalive configuration on the tunnel and to reload the configuration again; after the router has rebooted when the tunnel interface is still down.

- CSCtc38036

  The file table overflow error will occur when the file system is being accessed. This will occur after a few days on the ASR 1000 Router Series when running 2.4.1 and 2.4.2:

  router#more system:running-config

  %Error opening system:running-config (File table overflow)

  Workaround: Reloading the router solves the problem, but it appears again after a few days.

- CSCtc38484

  The giga word counters are not reflecting properly in the stop record.

  Workaround: There is no issues when the interim record is enabled. When the interim accounting is disabled on the ASR 1000 router, execute the **show interface virtual** command. This will allow for the giga word counter in the stop record to be confiigured.

- CSCtc40677

  When the distribute list is applied to the virtual template the distribute-list applied to the virtual-template interface is not effective for the virtual-access interfaces spawned by that template.For example, when the ASR 1000 router (hub) is configured as:

```
router eigrp 1
 redistribute static metric 10000 100 255 1 1500
 network 10.0.0.0
 no auto-summary
 distribute-list prefix TEST out Virtual-Template1!
ip route 0.0.0.0 0.0.0.0 Null0
ip route 10.0.0.0 255.0.0.0 Null0!
ip prefix-list TEST seq 10 permit 0.0.0.0/0
ip prefix-list TEST seq 20 permit 10.0.0.0/8
```

  For example:on the branch site when connected to a Virtual-accessinterface will show as:

```
ranch#sh ip route eigrp
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, *15:56:44.397 BRU Wed Oct 7 2009
10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D       10.0.0.0/8 [90/46251776] via 10.12.0.2, 00:00:06, Dialer1
D       10.1.1.0/24 [90/46228736] via 10.12.0.2, 00:00:06,Dialer1
D       10.2.2.0/24 [90/46354176] via 10.12.0.2, 00:00:06, Dialer1
D*EX 0.0.0.0/0 [170/46251776] via 10.12.0.2, 00:00:06, Dialer1
```

  For example: note that there is no filtering applied.

  In rare conditions this error may have occurred on the ASR 1000 router (hub) running 12.2(33)XND1 or later releases.

Workaround: Is to configure the distribute-list for the specific virtual-access interface used for the connections on the hub.

- CSCtc45743

  When VPN is configured between two ASR 1000 routers the traffic is encrypted, however when it reaches the end of the tunnel it is not decrypted. The flowing debug output is expected from “debug crypto ipsec”

  The IPSec configuration: (crypto_ipsec_create_transform_sas): Failed to attach flowid to hw

  In rare conditions this error may appear when the VPN tunnel has been created between two ASR 1000 routers on the RP2's and ESP20's running 2.4.1 and 2.4.2.

  Workaround: Reloading the router solves the problem,

- CSCtc45832

  When tracking stops the data-plane logs out of the PKT-MEM trace log this problem will occur on the ASR 1000 Router Series the sessions will be dropped and the QoS hierarchy will shut down. There also will be pending queue objects waiting to be flushed out in the list.

Note The following command will show the BQS RM status:

show plat hard qfp act inf bqs stat

In rare conditions, an error may occur for extreme over-subscribed enviroments. When sending 10G (For example: 5G as priority, and 5G as non-priority) traffic to a 1G interface.

All priority and control packets are dropped by the hardware this occur when the packet buffers are depleted; and when the schedule stops forwarding output packets

Workaround: There is no known workaround to this problem.

- CSCtc51048

  On the Cisco ASR 1000 Router the FP will reset, when configuring **show platform hardware cpp feature ipsec spd all** on the cli, after deleting tunnels FP crash on **sh pla hard cpp feature ipsec spd all** while deleting tunnels. This condition will occur when tunnel has been deleted and applyed to the CLI **show platform hardware cpp feature ipsec spd all** both even should happen together.

  Workaround: Do not apply CLI **show platform hardware cpp feature ipsec spd all** while you are deleting number of tunnels.

- CSCtc59162

  When modifying the prefix-list when configured as an inbound or outbound distribute-list does not trigger a resync of the EIGRP peer. This condition happens whe the Prefix-list has been has EIGRP as an inbound or outbound distribute-list.

  Workaround: To soft: clear the neighbor; and soft: clear ip eigrp neighbor <INTF_NAME>.

- CSCtc72899

  On the ASR 1000 Router Series does allow for abbreviated interface names this should be accepted by platform commands.

  Workaround: None

- CSCtc75736

  When EIGRP is configured on the ASR 1000 Router Series the MVPN Hub role stops sending acknowledgements for reliable packets. This condition on occurs when GRE Multipoint Tunnel shut/no shut has been applied.

Workaround: None

- CSCtc86951

  On the ASR 1000 Router Series, when high speed logging is enabled for NAT, ESP may fail after a RP SSO switchover. In rare conditions when high speed logging is enabled for NAT, ESP may fail after a RP SSO switchover.

  Workaround: None

Resolved Caveats—Cisco IOS XE Release 2.4.2

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.4.2

- CSCsc91697

  When DBS is applied Values (such as PCR, SCR and MBS) are not synced to standby. In rare conditions, an error will occur when DBS applied Values (such as PCR, SCR and MBS) are not synced to standby

  Workaround: None

- CSCse53019

  The BGP prefixes that should be redistributed to an IGP are not redistributed. When a route-map is used on the redistribution from BGP to the IGP and in the route-map statements such as **'match as-path...'or 'match community**..'are used to deny/allow networks to be redistributed. The network is initially received by BGP with an as-path/community that is denied by the route-map and later on the as-path/community changes which should allow it through the route-map but this never happens. The other way around is also affected, thus initially the BGP prefix being allowed but then later having a prefix in the BGP/routing table that should NOT be redistributed in the IGP but is being redistributed.

  Workaround: Is to'clear ip route <prefix>' or 'clear ip route * ' will trigger redistribution checking. Alternatively BGP table maps can be used to set tag and to redistribute based on tag and not on as-path/community.

  Further Problem Description: When certain attributes such as as-path or communities for an existing BGP prefix change, the routing table is updated but redistribution is never called so if redistribution from BGP to IGP's is based on a route-map which uses match community/match as-path statements then they will never be re-evaluated. This can lead to routing loops or blackholes.

  Workaround: None

- CSCsq03955

  On the ASR 1000 Router Series there are certain comands, such as **show platform hardware qfp act stat drop | ex _0_,** when executed on the newly active FP after the previously active FP was removed, may crash the smand process. The smand process crash does not result in the router crashing.

  When the RP is configured it resets to do shut/no shut on mlppp interfaces. This conditions occurs when s**hut/no shut** on mlppp interfaces, RP is reset on the ASR 1000 Router.

  Workaround: None

- CSCsq11897

  When BGP is configured on the ASR 1000 Router Series the system will crash when the interface board is removed. This rare condition is when BGP session is established and the corresponding interface board is removed.

Workaround: None

- CSCsr88898

  When spurious memory access may occur for scaled ppp sessions. In rare conditions an spurious memory access seen on clearing l2tp tunnel with scaled ppp sessions happens.

  Workaround: No workaround

- CSCsu46644

  When the ASR 1000 Router Series has rebooted you will no longer recieve username/password prompt until standby RP reaches SSO mode. The msg **%authentication failed** is received instead of router login prompt.

  Workaround: Add **no aaa account system guarantee-first** configuration.

- CSCsu52800

  When vrf configured has been configured (more than 1000 in this case), MCASTRED-3-DDE_REPLAY_FAILSAFE error message is displayed.

  Workaround: Is to increase the timeout of the PIM NSF Data Driven Event failsafe timer to resolve the problem.

- CSCsu82879

  After L4 redirect to broadhop SME portal, and with multiple subscribers trying to login into web server, the ASR1000 will popup with the following traceback:

  *Sep 29 11:11:40.830: %AAA-6-BADHDL: invalid hdl AAA ID 0, hdl 36020B6A, retired -Process= "SG CMD HANDLER", ipl= 0, pid= 151

  -Traceback= 1#afef50968b0f2116fc04276aae0dfa03 :10000000+50CA84 :10000000+50AC9C :10000000+50AF6C :10000000+40EB7C :10000000+418E98 :10000000+7E13A4 :10000000+7E125C :10000000+283889C :10000000+2833B64 :10000000+28353F0

  Workaround: None

- CSCsv91587

  The **aaa authorization** command, the **aaa authorization network default if-authenticated** only one session is coming up. The user receives authorization failures on the cli once log onto a device on the TACACS server; it is unreachable when logged in with their local credentials.

  Workaround: As the issue is specific to "if-authenticated" part in aaa authorization configuration [aaa authorization exec default group tacacs if-authenticated], the following configuration could be used as a workaround: [aaa authorization exec default group tacacs local]

- CSCsw31028

  The file type is mismatched in "show slot0:" and "show file info" output and the incorrect file type has been displayed for unicode file in show slot 0. This happens on the ASR 1000 Router Series when executing show slot0: it shows file type as config for unicode file.

  Workaround: None

- CSCsx06457

  The ASR 1000 Router Series when BGP is configured it may generate IPRT-3-NDB_STATE_ERROR log messages. An additional symptom when **bgp suppress-inactive** is configured is that the router CPU usage may get close to 100%. In rare conditions when both BGP and an IGP are advertising the same prefix, an error may occur. In addition **bgp suppress-inactive** command is configured with high CPU usage.

Workaround: Removing the **bgp suppress-inactive** configuration should eliminate the high CPU usage. Alternative option is to remove BGP or IGP conflicting routes from the system.

- CSCsx08861

  On the ASR 1000 Series the AToM VC status is seen as down in standby RP and traffic loss is seen after switchover for 44 seconds.

  Workaround: There are two work arounds for this issue:

  1. Do not reconfigure the ATOM VC immediately after deleting a subinterface.
  2. Do not copy and paste the ATOM VC

  Either do it manually step by step or copy the config from file.

- CSCsx29726

  On the ASR 1000 series router when the fail-close is unconfigured and the GDOI crypto map is in fail-close mode (after an unsuccessful registration), the crypto map will drop all unencrypted traffic regardless of a subsequent successful registration. On the ASR 1000 series router if fail-close is unconfigured when a GDOI crypto map is in fail-close mode (after an unsuccessful registration), the crypto map will drop all unencrypted traffic regardless of a subsequent successful registration. For this condition the symptom is observed when a GDOI crypto map configured with fail-close. Fail-close is unconfigured while crypto map is in fail-close mode.

  Workaround: Is to remove and reapply the crypto map to the interface or the fail-close configuration.

- CSCsx63700

  On the ASR 1000 Series the L2TP PMTU reset timeout, the Vaccess interface MTU is not restored to its original configured MTU. The old MTU value which was PMTU has been left on. On the ASR 1000 Serie this rare condition that will happen only on the VPDN LNS and when L2TP Path MTU is configured, and after a PATH MTU reset timeout.

  Workaround: None

- CSCsx90419

  ASR 1000 Router Series when policy is configured with excess bandwidth as well as queue-limit feature. In rare conditions when policy is confirgured on mfr interface the policy gets rejected instead of suspended.

  Workaround: None

- CSCsy07953

  On the ASR 1000 Series Router any attempt to copy a file from a router to an FTP server this will fail. On the FTP server the error is **No such file or directory.** For this rare condition the ASR 1000 Router Series has a problem with FTP when transferring files to an FTP server.

  Workaround: Is to use a different file transfer protocol, such as TFTP

- CSCsy08167

  On The ASR 1000 Router Series when auto re-enroll is started or a manual re-enroll is attempted for a certificate when Certificate Authority (CA) is using a manual grant method, the router will retry based on the default or configured retry counts and intervals. When the maximum retries are exceeded and the renewed certificate is not received from CA, the current certificate which is not yet expired, and this is not available until a reload.

  For the new IKE negotations using the **cypto pki authenticate ca** will fail with following message:

```
Feb 27 14:25:56.615: CRYPTO_PKI: Can't find signature certificate for
trustpoint
Feb 27 14:25:56.615: ISAKMP (7002): unable to build cert chain
```

```
Feb 27 14:25:56.615: ISAKMP (7002): FSM action returned error: 2
Feb 27 14:25:56.615: CRYPTO_PKI:
```

Workaround: There are two work around for this issue.

1. Is to increase the enrollment retries and count
2. Is to reload the router

- CSCsy16177

  On the ASR 1000 Series Router may experience invalid checksum over SCP on SSH version 2. This rare conditions may a occurs on a On the ASR 1000 Series Router with flash type file system.

  Workaround: There is no workaround.

- CSCsy19463

  On the ASR 1000 Series Router when NHRP has been configured as a mGRE tunnel interface configuration is related to NHRP/DMVPN the router may fail.

  Workaround: There is no workaround.

- CSCsy20343

  On the ASR 1000 Series Router may hang or bus error may cause a failure when polling CISCO-CLASS-BASED-QOS-MIB. In rare instances the ASR 1000 Router Series may fail when polling OID: 1.3.6.1.4.1.9.9.166

  Workaround: Is to Exclude OID: 1.3.6.1.4.1.9.9.166 or to disable SNMP.

- CSCsy22311

  When using secure copy (SCP) the ASR 1000 Router Series this may cause compatibility issues. In rare, conditions this may occur when using SCP SSH version 2 on the ASR 1000 Router Series.

  Workaround: None

- CSCsy33068

  On the ASR 1000 Series Router when the SDP HTML template are between 1KiB and 10KiB this may cause an abrupt termination of the SDP process. In rare instances the HTTP post to the HTTP server in an On the ASR 1000 Series Router is size-limited. The limit is set to 32KiB by default. In the SDP process, the transition from introduction page to the completion page involves an HTTP post. The post contains information including the SDP bootstrap configuration and the completion template together with the overhead of HTTP post communication. The size limit might be reached with moderate usage of HTML elements. The HTTP post in SDP is base-64 encoded. The total size limit of the SDP bootstrap and the completion template is roughly (32KiB - 2KiB(overhead))* 3/4(base-64 encoding) = 22.5KB.

  Workaround: Is to reduce the size of the HTML template, and abridge the configuration. The total size of the two cannot exceed ~22.5KB.

- CSCsy34538

  On the ASR 1000 Series Router after crypto PKI certiificate has been reloaded the certificates are not loaded from the USB Token when the reload of router certificates are not stored, or there not available on the Alladin USB token.

  Workaround: Is to copy certificate files from the usbtoken0: device into the nvram: filesystem and then configure **crypto pki certificate storage nvram.**

- CSCsy40745

When disabling SSH, an alternate SSH port this is still enabled on the ASR 1000 Series. This condition may occur on the ASR 1000 Series when has been configured to use a port other than Port 22 for SSH.

Workaround: Do not configure alternate SSH ports.

- CSCsy41887

  On the ASR 1000 Router Series an error message on console, or some traffic may drop when the ESP20 is configured for IPSec.

  Workaround: None

- CSCsy42850

  On the ASR 1000 Series Router when CNS is configure a memory leak may occur when using memory leak debug tool.

  Workaround: Is to not configure **cns**.

- CSCsy44755

  When IPv6 configuration is blocked when xconnect is configured for the interfaces on the ASR 1000 Router Series. This condition may be rare only when xconnect is configured for any interface on the ASR 1000 Router Series.

  Workaround: None

- CSCsy53445

  On the ASR 1000 Router Series the SDP server may fail on **crypto pki enroll <trustpoint>.**

  Workaround: None

- CSCsy79955

  On the ASR 1000 Router Series reverse SSH using PVDM2 modems may fail. If the **ssh -l <username>:<line #> <ip> command is entered,** and modem activation is triggered. The input of **atdt<number>** is making it to the modem, meaning whatever the <number> field is typed, it is reported in the debugs. However, the modem does not send anything back to router about it and no connection is made. At modem prompt, **at**, **at&f**, **ate1** (and perhaps others) do not appear to be taken.

  Workaround: Is to configure **ssh** (only)on the router,afterwards issue a **reverse** telnet

- CSCsy88034

  On the ASR 1000 Router Series the **flow data** in the **show ip cache [***verbose***] flow** commands output maybe missing. This condition may occurs when there is churn from netflow related configuration; especially exported configuration that are toggling **flow (enabling/disabling),** flapping of interface enabled with netflow.

  Workaround: Is to reload the router.

- CSCsy88764

  On the ASR 1000 Router Series the ISG PPPOE sessions may lose authenticated state if they receive Change of Authorization (COA) for service swapping. In rare instances when sending COA pushes to deactivate an existing service and active new one to ISG PPPOE sessions, the sessions may change state from authenticated to connect to the sessions that are already in logoff state. As a result, all Subscriber Service Switch (SSS) showings are empty.

  Workaround: None

- CSCsy90542

On the ASR 1000 Router Series the Multicast traffic is dropped at decrypting side. In rare conditions this symptom will occur when traffic ACL on the KS is of this type: permit **show ip host** *address* **show ip host** *any permit* **show ip host** *ip any host* **show ip host** *address* commands.

Workaround: There is no workaround.

- CSCsy92808

  On the ASR 1000 Router Series the certificate verification failure result is not returned to the client application(for opssl), instead a generic error is sent. This may be visible when SSLVPN and a connection to the back-end server is established via https, the page does not open and the browser hangs.

  Workaround: None

- CSCsy95838

  When external storage is configured on the ASR 1000 Router Series, the CRL may not be updated even if current CRL validity expires.

  Workaround: There are two workarounds for this issue:

  1. **shut/no shut** the crypto pki server.
  2. Increase the lifetime of CRL to maximum (2 weeks)
  3. Disable CRL checking

- CSCsy98000

  When IOS is configured on the ASR 1000 Router Series there maybe a failure when issuing **reload** command. In rare conditions, the ASR 1000 Router Series may fail on occasion if there are a large amount of messages that are to be printed on the IOS console.

  Workaround: Before reloading the router, disable console logging by giving the command **no logging console** from the configure mode. (or) Before reloading disable the watchdog issue the command **test platform software infrastructure watchdog off.**

  Instead of performing the above manual steps before each reload, please configure **logging reload errors** so that only more severe log messages are allowed to be printed on console during device reload.

- CSCsz02499

  When an Ethernet SPA interface with QinQ sub-interface configuration is disabled and then enabled, an error message about failing to apply PLIM input classification on the Ethernet SPA is displayed on the console. This condition is rare when QinQ sub-interface is configured on an Ethernet SPA on the ASR 1000 Router Series. The "show running-config" command is executed and then the Ethernet SPA interface is disabled and then enabled.

  Workaround: There is no functionality impact due to this error message. The QinQ sub-interface should be able to successfully pass traffic.

- CSCsz11759

  On the ASR 1000 Router Series the certificate enrollment process may fail for software crytpo engine.

  Workaround: None

- CSCsz22129

  On the ASR 1000 Router Series the class-maps in a QoS service-policy may get re-ordered by getting moved to the end of the policy-map. On the ASR 1000 Router Series this is arare condition the has been seen when the class-map is modified by adding new filters or modifying existing filters in the class-map.

Workaround: None

- CSCsz22367

  On ASR 1000 Router Series during a removal of BGP config with 'no router bgp' being copied from saved config file to running config.

  Workaround: None

- CSCsz26610

  On the ASR 1000 Router Series unexpected system reload may occur when "crypto pki authenticate CA" is configured with a certificate that is missing keyUsage = cRLSign. In rare instances when **crypto pki authenticate CA** command is configured with a certificate that is missing keyUsage = cRLSign a system reload may occur.

  Workaround: Is to configure "crypto pki authenticate CA" with a certificate that is includiing keyUsage = cRLSign.

- CSCsz27200

  Although the **show ip route** *ip-address* command is supported, the *ip-address* (or A.B.C.D.) option and its related parameters do not appear in the auto-completion list when the "?" or help prompt is entered for the **show ip route** command on a Cisco ASR 1000 Series Router.

  For example, note that the *ip-address* option does not appear in the list of subcommands below:

```
Router# show ip route ?
  bgp             Border Gateway Protocol (BGP)
  connected       Connected
  dhcp            Show routes added by DHCP Server or Relay
  eigrp           Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis            ISO IS-IS
  list            IP Access list
  loops           RIB routes forming loops
  mobile          Mobile routes
  multicast       Multicast global information
  odr             On Demand stub Routes
  ospf            Open Shortest Path First (OSPF)
  profile         IP routing table profile
  rip             Routing Information Protocol (RIP)
  static          Static routes
  summary         Summary of all routes
  supernets-only  Show supernet entries only
  topology        Display routes from a topology instance
  track-table     Tracked static table
  vrf             Display routes from a VPN Routing/Forwarding instance
  |               Output modifiers
```

  In addition, no list of optional parameters appear if the "?" or help prompt is entered following the **show ip route** *ip-address* command as shown below:

```
Router#sh ip route 10.1.1.1 ?
% Unrecognized command
```

  But the **show ip route** *ip-address* command is supported and works as expected:

```
Router#sh ip route 10.1.1.1
Routing entry for 10.1.1.1/32
  Known via "ospf 1", distance 110, metric 2, type intra area
  Last update from 10.0.0.3 on GigabitEthernet0/3/2, 4d01h ago
  Routing Descriptor Blocks:
    172.16.0.3, from 10.1.1.1, 4d01h ago, via GigabitEthernet0/3/2
      Route metric is 2, traffic share count is 1
```

```
  * 10.0.0.3, from 10.1.1.1, 4d01h ago, via GigabitEthernet0/3/0
      Route metric is 2, traffic share count is 1
Router#sh ip route 10.1.1.1 | in ospf
  Known via "ospf 1", distance 110, metric 2, type intra area
```

Workaround: None

- CSCsz45761

  When the SIP is configured on the ASR 1000 Router Series the messages can be dropped: - 200-OK - 183-SESSION-PROGRESS - 180-RINGING - ACK. In rare instances, the CONTACT header in the INVITE/200/183/180/ACK message may not have a port number specified on the ASR 1000 Router Series.

  Workaround: None

- CSCsz66842

  When Proxy service logon is configured it passes a wrong username on the ASR 1000 Router Series. In rare conditions the ASR 1000 Router Series when verifying the Tests for TC-Proxy, a service logon is performed with correct and incorrect username. When using incorrect Username, proxy service logon gets successfully applied as seen in the output of "show subscriber session all" even when Authentication gets rejected.

  Workaround: None

- CSCsz68932

  If a user enters an ambiguous command in adjacency sip submode on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) then the system leaves the prompt at the parent config-sbc-sbe level.

  For example, in the following sequence the user enters the ambiguous “re” command:

  ```
  Router(config-sbc-sbe)# adjacency sip client
  Router(config-sbc-sbe-adj-sip)# re
  % Ambiguous command:  "re"
  ```

  Now if the user tries to go back into the adjacency sip submode, the following error is displayed and the mode does not change:

  ```
  Router(config-sbc-sbe)#adjacency sip client
  Failed to access SBE cli configuration. Unable to execute command.
  ```

  Workaround: Exit the config-sbc-sbe submode to the config-sbc level. Then re-enter adjacency sip submode using the **sbe** and **adjacency sip** configuration commands as follows:

  ```
  Router(config-sbc-sbe)# exit
  Router(config-sbc)#sbe
  Router(config-sbc-sbe)#adjacency sip client
  Router(config-sbc-sbe-adj-sip)#
  ```

- CSCsz71478

  When there are a larger number of interfaces configured on the ASR 1000 Router the following traceback may appear:

  ```
  %AAA-3-BADLIST: invalid list AAA ID 11 -Process= "Exec", ipl= 0, pid= 76
  ```

  On rare conditions the trace-back may occur during boot-up time when there are a large number of interfaces configured on the ASR 1000 Router Series.

  Workaround: None

- CSCsz71654

When Accounting Records is configured on the ASR 1000 Router Series this may not show the correct username when the Web authenticated identifier uses IP addresses for routed IP sessions. In rare instances when on the ASR 1000 Router Series the account-logon (authentication) happens after failed Transparent Auto-Logon (TAL).

Workaround: None

- CSCsz72022

  The Cisco ASR 1000 Series Router crashes when a DBE command is entered on one line, and immediately after on another line, the SBC configuration is removed (for example, **no sbc** *name*). This text is similar to the following that is printed on the console, and then the router reloads.

  ```
  SBC: Assertion failed - csb->nvgen
  SBC: at ../sbc/sbc-infra/src/ios_cli/sbc_dbe_config.c:4323
  ```

  Workaround: Do not configure SBC on multiple lines simultaneously.

- CSCsz72973

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when malformed H.323 packets are received at a high rate and an Embedded Services Processor (ESP) switchover is in progress.

  This problem is intermittent

  Workaround: None

- CSCsz76450

  The Cisco ASR 1000 Router Series **show memory** *ip address* command may not allow for output.

  The console may return the following error message:

  % Invalid input detected at '^' marker

  In rare instances this may occur on a 64-bit Cisco ASR 1000 Router running in 2.3.0 or 2.4.0 releases.

  Workarond: None

- CSCsz77311

  Crash occurs in mfib_db_table_is_downloadable(). This issue may be seen when the following configuration command is issued:

  no ipv6 multicast-routing

  Workaround: None

- CSCsz91269

  The Cisco ASR 1000 Router Series may receive an error message return on the IOS console indicating a failure when downloading the correct NAT configuration from RP to CPP.

  This text is similar to the following that is printed on the console **ERR: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: DYN-MAP: map_id 11 download to CPP"**

  Workaround: None

- CSCta00591

  The memory leak has been seen on the ASR 1000 Router Series when the router is configured to download lists or filters.

  Workaround: None

- CSCta06282

The Cisco ASR 1000 Router Series will do a check on whether the packet forwarding is working fine however there may be a rare instance when, the counters are not incrementing.

When turning on the **debug platform software multicast stat** this text is similar to the message n the console:

Jun 8 11:55:53.334: FMANRP-MCAST: M_ID 0 is not associated with an entry

The following message in this text that is similar to what may happen for special route combinations:

ipv6 mld static-group FF03::2:1:1

ipv6 mld static-group FF03::1:1:2

Workaround: To do group address changes.

- CSCta08194

  In rare instances the ASR 1000 Router Series may fail when reprovisioning AToM Tunnel with AAL5 Encapsulation.

  Workaround: None

- CSCta08772

  When EzVPN clients are failing negotiations on the ASR 1000 Router Series this may cause the router to use the less-specific route. In rare conditions the problem can occur when 0/0 is configured as a destination and EXACT_MATCH is specified.

  Workaround: None

- CSCta12296

  The Group Member crashes on the Cisco ASR 1000 Series Routers. In rare instances this occurs when unicast re-keys are received frequently (TEK 300).

  Workaround: None

- CSCta12360

  The Cisco ASR 1000 Series Router NAT Limit count may be falsely set to 0.

  This rare instance happens in lower traffic conditions when issuing **clear ip nat trans** after changing the limit maximum value.

  Workaround: Do not issue **clear ip nat trans** before changing maximum count for a limit.

- CSCta15960

  Spurious memory access followed by a traceback are logged on the ASR 1000 Series Router. In this rare condition the ASR 1000 Series Router is enrolling as a certificate server for the first time with GETVPN configured.

  Workaround: There is no workaround.

- CSCta22703

  The Cisco ASR 1000 Series Router has a problem that the 'agent address' field for coldstart and link down TRAP is notified as ip address of vlan1(shutdown).

  Workaround: To do snmp-server source-interface traps vlan "source vlan#" is set

- CSCta33240.

  CPP QoS EA encountered an error on the ASR 1000 Router Series. In this condition when an hierarchy policy-map is attached to the interface on both the input and output directions, after reloading the system by removing the policy-map without detaching it from the interface, an error message will occur on the console.

Workaround:Detach the policy-map from the interface then remove the policy-map.

- CSCta41084

  Packets encrypted and decrypted are not incrementing at the hub end after rekey. The issue is seen on a DMVPN head end aggregating 1000 spokes after the rekey timer has expired.

  Workaround: None

- CSCta57125

  Netflow statistics stopped updating after several instances of toggling between full and random sampled mode.

  Workaround: Do not toggle between full and random sampled Netflow mode.

- CSCta59045

  When the 32K dual stack sessions is configured on a PTA device (ASR1000 Series Router) with another ASR1000 client using the **test pppoe"**command, the client crashes with an IOS crash when 14K sessions comes up on the PTA. The ASR 1000 client crashes while in this condition, **test pppoe** command is configured, while trying to bring up 16K dual stack sessions on a PTA device and both the PPPoE client and PTA are ASR 1000 clients.

  Workaround: None

- CSCta63406

  In this condition when debug is used with **xconnect logging pseudowire status** the ADVIPSERVICESK9 image is unable to see **%XCONNECT-5-PW_STATUS** log message in the console.

  Workaround: None

- CSCta65367

  In this condition **show sbc** and **sbe call** commands will display call type as Audio.

  Work around: None

- CSCta65822

  When a switchover occurs on the ASR1000 Router Series for L2TP LAC thousands of sessions with tunnels are being disconnected, in some instances some sessions will be left in a "stale" state on the newly active RP. Apart from memory wastage, there is a functionality impact too future sessions with tunnels with the same session with tunnel ids as these stale sessions may be rejected.

  Workaround: Is to clear these stale sessions by using any clear commands. As a possible workaround is to ensure that all tunnels complete resync successfully by ensuring that either all sessions in it are not being disconnected at the same time that a switchover occurs OR by configuring "**l2tp tunnel timeout no-session <high value/never>"** on both LAC and LNS so that tunnel stays up even after there are no more sessions in it (so that it can complete successful resync).

- CSCta68936

  QoS VSA 1 attributes are not included in the service accounting record for complex QoS parameterized service.

  Work around: None

- CSCta72981

  In some conditions when creating a configuration view with **command parse view** this will not work, when **command configure** includes all **class-map type inspect.**

  Work around: None

- CSCta74405

When authentication is not configured in the transform-set, the output of IPSec SA shows anti-replay is disabled, but out of order packets are dropped once the default anti-replay window of 64 packets are reached.

Workaround: Is to disable anti-replay manually or increase the anti-replay window.

- CSCta86988

  The Cisco ASR 1000 Router Series will reload when using **debug sbc SBC-PE2 filter sip call** and **debug sbc SBC-PE2 filter call.**

  Workaround: Avoid enabling both debugs during critical call flow with this issue present.

- CSCta95969

  NAT pool address depletion occurs when running using PAT with pure IP traffic on the ASR 1000 Router Series.

  Workaround: Is to configure ACL to drop with pure IP traffic on NAT inside all interfaces.

- CSCta96311

  Decrypted IPSec packets are not forwarded to the IVRF with dual ISPs, when the primary default route has a higher number of interfaces with crypto mapping applied.

  Workaround: Is to use the command **no ip route-cache cef** on the ingress interface for incoming IPSec packet.

- CSCtb34308

  In rare conditions tracebacks are seen when initiating 4000 sessions on LNS on the Cisco ARS 1000 Router Series.

  Workaround: None

- CSCtc60363

  QoS queue-limit update does not work with qos fair-queue on the ASR 1000 Router Series, when configuring qos fair-queue and qos queue-limit in policy-map.

  Workaround: Is to change qos queue-limit before applying policy-map to interfaces.

Open Caveats—Cisco IOS XE Release 2.4.1

This section documents possible unexpected behavior by Cisco IOS XE Release 2.4.1.

- CSCse53019

  BGP prefixes that should be redistributed to an IGP are not redistributed.

  A route-map is used on the redistribution from BGP to the IGP and in the route-map statements such as ‘match as-path... or match community...' are used to deny/allow networks to be redistributed. The network is initially received by BGP with an as-path/community that is denied by the route-map. Later on the as-path/community changes which should allow it through the route-map but this never happens.

  The other way around is also affected. Thus initially the BGP prefix is allowed but then later having a prefix in the BGP/routing table that should *not* be redistributed in the IGP but is being redistributed.

  Workaround: The commands **clear ip route** *prefix* or **clear ip route *** will trigger redistribution checking. Alternatively BGP table maps can be used to set the tag and to redistribute based on the tag and not on as-path/community.

- CSCsw65614

Network Address Translation (NAT) is used with route maps with a SUP720 and some specific combinations of IP address, vlan# as outside interface, NAT for TCP application does not work correctly. With this issue, the extended VLAN is used for the outside interface, and the interface IP address matches the pool IP address.

Workaround: Use the **ip nat inside source route-map** *route-map* **interface** *interface* **overload** command as a substitute for **ip nat inside source route-map** *route-map* **pool** *pool* **overload** command.

- CSCsx61017

  Linecard switchover time is greater than expected. The error message is:

  ```
  error_msg = Switchover time is 70.631028 seconds, and expected is  1.5  seconds
  ```

  The issue occurs with all line cards. The issue is reproducible with a script only.

  Workaround: None

- CSCsx08861

  When an Any Transport over MPLS (AToM) virtual circuit (VC) subinterface is removed and then recreated (reprovisioned) on a Cisco ASR 1000 Series Router, the VC status on the standby RP should show as "HOTSTANDBY," but it shows as "DOWN." If a forced switchover is executed using the **redundancy force-switchover** command, the VC experiences about 44 seconds of traffic loss.

  Workaround: There are two possible workarounds for this issue.

  1. Do not reconfigure the AToM VC immediately after deleting the subinterface.
  2. Do not copy and paste the AToM VC configuration. Either do it manually step by step or copy the configuration from file.

- CSCsy19417

  When the number of Border Gateway Protocol (BGP) prefixes exceeds 300K in a Layer 3 VPN (L3VPN) scenario on a Cisco ASR 1000 Series Router and a reload is executed, Cisco Express Forwarding (CEF) is disabled. Before the reload, CEF functioned even though there were as many as 400K prefixes

  Workaround: None

- CSCsy49927

  The IOSd process restarts and returns the following error message:

  ```
  %Error opening tftp://202.153.144.25/hprem/rtr_crest.exp (Timed out)
  ```

  Workaround: None

- CSCsy73014

  On a Cisco ASR 1000 Series Router, the Internet Protocol Communications (IPC) RX flow control signals do not function properly. Traffic in excess of the IPC RX rising threshold will trigger the IPC RX STOP signal. However, when traffic levels drop below the falling threshold, the IPC RX START signal will not be sent.

  Workaround: None

- CSCsz01980

  Under very rare conditions, an RP1 on a Cisco ASR 1000 Series Router may experience an unexpected watchdog timeout during boot or shutdown and reload.

  Workaround: None

Following the reload, the RP1 works as expected.

- CSCsz18138

  Removing IPv4 or IPv6 addresses from VRF interfaces on a Cisco ASR 1000 Series Router results in traceback.

  Workaround: None

- CSCsz24683

  Shutting down subinterfaces configured with bidirectional forwarding detection (BFD) results in traceback.

  Workaround: None

- CSCsz24818

  When the **ip telnet source interface** command is configured to point at an interface that has an IPv6 address on a Cisco ASR 1000 Series Router, the RP resets.

  Workaround: Do not use the **ip telnet source interface** command.

- CSCsz25573

  When the pado delay parameter is configured under 4000 bba-groups on a Cisco ASR 1000 Series Router configured as an L2TP Access Concentrator (LAC), the following error message appears repeatedly at the router:

  ```
  %AAA-3-ACCT_LOW_MEM_UID_FAIL: AAA unable to create UID for incoming calls due to
  insufficient
  ```

  If the configuration is saved to NVRAM, the router reloads repeatedly after a reboot

  Workaround: If the pado delay configuration is only applied to 1000 bba-groups, the problem does not occur.

- CSCsz26610

  An unexpected system reload occurs when the **crypto pki authenticate CA** command is configured on a Cisco ASR 1000 Series Router with a certificate that is missing keyUsage = cRLSign.

  Workaround: Configure the **crypto pki authenticate CA** command with a certificate that includes keyUsage = cRLSign.

- CSCsz27068

  Under rare conditions, Open Shortest Path First (OSPF) may reset when the interfaces on a Cisco ASR 1000 Series Router are unconfigured in a very short interval.

  This condition is caused by a timing issue in OSPF.

  Workaround: None

- CSCsz27200

  Although the **show ip route** *ip-address* command is supported, the *ip-address* (or A.B.C.D.) option and its related parameters do not appear in the auto-completion list when the "?" or help prompt is entered for the **show ip route** command on a Cisco ASR 1000 Series Router.

  For example, note that the *ip-address* option does not appear in the list of subcommands below:

  ```
  Router# show ip route ?
    bgp             Border Gateway Protocol (BGP)
    connected       Connected
    dhcp            Show routes added by DHCP Server or Relay
    eigrp           Enhanced Interior Gateway Routing Protocol (EIGRP)
    isis            ISO IS-IS
    list            IP Access list
  ```

```
  loops           RIB routes forming loops
  mobile          Mobile routes
  multicast       Multicast global information
  odr             On Demand stub Routes
  ospf            Open Shortest Path First (OSPF)
  profile         IP routing table profile
  rip             Routing Information Protocol (RIP)
  static          Static routes
  summary         Summary of all routes
  supernets-only  Show supernet entries only
  topology        Display routes from a topology instance
  track-table     Tracked static table
  vrf             Display routes from a VPN Routing/Forwarding instance
  |               Output modifiers
<cr>
```

In addition, no list of optional parameters appear if the "?" or help prompt is entered following the **show ip route** *ip-address* command as shown below:

```
Router# show ip route 3.3.3.3 ?
% Unrecognized command
```

But the **show ip route** *ip-address* command is supported and works as expected:

```
Router# show ip route 3.3.3.3
Routing entry for 3.3.3.3/32
  Known via "ospf 1", distance 110, metric 2, type intra area
  Last update from 63.0.0.3 on GigabitEthernet0/3/2, 4d01h ago
  Routing Descriptor Blocks:
    63.0.0.3, from 3.3.3.3, 4d01h ago, via GigabitEthernet0/3/2
      Route metric is 2, traffic share count is 1
  * 36.0.0.3, from 3.3.3.3, 4d01h ago, via GigabitEthernet0/3/0
      Route metric is 2, traffic share count is 1
Router# show ip route 3.3.3.3 | in ospf
  Known via "ospf 1", distance 110, metric 2, type intra area
```

Workaround: The **show ip route** *ip-address* command actually is supported; its syntax just does not appear at the "?" or help prompt. For detailed information on the syntax for the **show ip route** *ip-address* command, see the following online documentation at Cisco.com:

http://www.cisco.com/en/US/partner/docs/ios/iproute/command/reference/irp_pi2.html#wp1015483

- CSCsz42939

  IOS crashes when the Cisco ASR 1000 Series Router has multiple interfaces configured with SPA-4XCT3/DS0/ SPA-2XCT3/DS0 SPA. Configuring multiple channel groups on SPA-4XCT3/DS0 SPA and performing a soft/hard OIR causes the router to crash. The router reloads.

  Workaround: None

- CSCsz47599

  The T3/E3 interface on a Cisco ASR 1000 Series Router does not come up after the router reloads.

  This condition is the result of a timing issue.

  Workaround: Execute a **shut/no shut** on the affected interface to bring the interface up.

- CSCsz54781

  Session interim accounting for PPP over X (PPPoX) sessions is not functioning in Cisco IOS XE Release 2.3.0 and later releases. When interim accounting is enabled on a per-session basis, no interim accounting updates get sent to the AAA server for PPPoX sessions.

  Workaround: None

- CSCsz56462

  The default behavior of the Cisco ASR 1000 Series Router is for the Cisco Discovery Protocol (CDP) to be disabled.

  Workaround: To enable CDP, include the **cdp enable** command in the configuration.

- CSCsz68932

  If a user enters an ambiguous command in adjacency sip submode on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) then the system leaves the prompt at the parent config-sbc-sbe level.

  For example, in the following sequence the user enters the ambiguous “re” command:

```
Router(config-sbc-sbe)# adjacency sip client
Router(config-sbc-sbe-adj-sip)# re
% Ambiguous command:  "re"
```

  Now if the user tries to go back into the adjacency sip submode, the following error is displayed and the mode does not change:

```
Router(config-sbc-sbe)#adjacency sip client
Failed to access SBE cli configuration. Unable to execute command.
```

  Workaround: Exit the config-sbc-sbe submode to the config-sbc level. Then re-enter adjacency sip submode using the **sbe** and **adjacency sip** configuration commands as follows:

```
Router(config-sbc-sbe)# exit
Router(config-sbc)#sbe
Router(config-sbc-sbe)#adjacency sip client
Router(config-sbc-sbe-adj-sip)#
```

- CSCsz72022

  The Cisco ASR 1000 Series Router crashes when a DBE command is entered on one line, and immediately after on another line, the SBC configuration is removed (for example, **no sbc** *name*). Text similar to the following is printed on the console, and then the router reloads.

```
SBC: Assertion failed - csb->nvgen
SBC: at ../sbc/sbc-infra/src/ios_cli/sbc_dbe_config.c:4323
```

  Workaround: Do not configure SBC on multiple lines simultaneously.

- CSCsz72973

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when malformed H.323 packets are received at a high rate and an Embedded Services Processor (ESP) switchover is in progress.

  This problem is intermittent

  Workaround: None

- CSCsz77311

  Crash occurs in mfib_db_table_is_downloadable(). This issue may be seen when the following configuration command is issued:

no ipv6 multicast-routing

Workaround: None

- CSCsz82587

  If Multi Protocol Label Switching Traffic Engineering (MPLS-TE) sessions come up or go down during online insertion and removal (OIR) on a Cisco ASR 1000 Series Router, the router may reload.

  Workaround: None

- CSCsz89484

  Blacklisting of a VPN does not take effect on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) for the following configuration:

  ```
  sbe
   blacklist vpn vpn-name
    reaason authentication-failure
     trigger-size 2
  ```

  The intended blacklisting action does NOT take effect because the trigger-period is NOT configured.

  Workaround: Configure the trigger-period using the **trigger-period** *num time-units* command.

- CSCsz94376

  When a very large number of calls are being processed through Cisco Unified Border Element (SP Edition) (CUBE) on a Cisco ASR 1000 Series Router and CUBE is deactivated and activated, an exception occurs and the router reloads.

  Workaround: None

- CSCta27191

  When using the command **upgrade rom-monitor filename harddisk:asr1000-rommon.XND.pkg** all for upgrading ROMmon, XND ROMmon failed to upgrade the RP1 board on 6RU(RP2) chassis.

  Workaround: None

- CSCta41084

  Packets encrypted and decrypted are not incrementing at the hub end after rekey. The issue is seen on a DMVPN head end aggregating 1000 spokes after the rekey timer has expired.

  Workaround: None

- CSCta45697

  When the total throughput of high priority and low priority IPsec traffic oversubscribed the encryption/decryption engine, high priority IPsec traffic is sometimes dropped.

  Workaround: Reduce the IPsec traffic bandwidth to below threshold.

- CSCta57125

  Netflow statistics stopped updating after several instances of toggling between full and random sampled mode.

  Workaround: Do not toggle between full and random sampled Netflow mode.

- CSCta37340

  The **show memory debug** command shows an increase in memory leaks at the IOSD ipc task as SPA modules are disabled/stopped one by one.

  Workaround: None

- CSCta74405

When authentication is not configured in the transform-set, the output for the IPSec Security Association (SA) shows anti-replay is disabled, but out-of-order packets get dropped once the default anti-replay window of 64 packets is reached.

Workaround: Disable anti-replay manually or increase the anti-replay window.

- CSCta76460

  IPSec EZVPN tunnels may be lost (not rekeyed properly) after a few rekey intervals.

  Workaround: Increase the rekey interval to the maximum to avoid the frequency of rekeying.

- CSCta86988

  The Cisco ASR 1000 Series Router crashed during Session Border Control (SBC) debug using a normal call.

  Workaround: None

- CSCtb01505

  While unconfiguring OSPF configurations, the Cisco ASR 1000 Series Router crashes with ospf_build_net_lsa.

  Workaround: None

- CSCtb01934

  System returns to ROMmon when booting IOS XE XND with a corrupted hard disk. If the filesystem on the hard disk is severely corrupted, IOS XE will fail to boot and return to ROMmon.

  Workaround: Booting an IOS XE XNC image will correct the filesystem errors, and any subsequent boot of IOS XE XND will be successful.

- CSCtb05335

  When tunnel protection IPsec is configured on a Generic Routing Encapsulation (GRE) tunnel, Label Distribution Protocol (LDP) session is flapping and the LDP neighborship on the GRE tunnel is going down.

  Workaround: To change tunnel protection, stop the traffic and then apply or remove tunnel protection.

- CSCtb05810

  When applying the **no distance** command, the summary-prefix disappears from the route table. When you check the ospfv3 database, the summary route exists.

  Workaround: Configure summary-prefix command again.

- CSCtb07984

  The Cisco ASR 1006 router acting as a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) failed to apply D2 QoS on the first two PPPoX sessions after every new reboot, but configures D2 QoS on all subsequent sessions.

  Workaround: LNS router configures D2 QOS on all subsequent sessions.

- CSCtb08490

  IPSecv6 tunnel fails to come up after tunnel protection is configured/unconfigured. The issue is seen when IPv6 traffic is flowing through the tunnel.

  Workaround: Stop the traffic before configuring/unconfiguring tunnel protection.

- CSCtb11807

Route Processor (RP) crash occurs when enablingIPv4 and v6 multicast routing and MPLS on the same interface. Multicast MPLS is not a supported mode for the Cisco ASR 1000 Series Router. The same interface requires all three features to be configured to cause the RP crash:

- IPv4
- IPv6
- MPLS
- ip sparse-dense mode

The following is a sample configuration:

```
interface GigabitEthernet0/3/2
 ip address 87.87.87.2 255.255.0.0
 negotiation auto
 ip sparse-dense mode   <<< will cause crash
 ipv6 address 2004:B010::6/64
 ipv6 ospf hello-interval 5
 ipv6 ospf 1 area 0
 mpls bgp forwarding
 cdp enable
end
```

Workaround: Do not configure MPLS on the same interface that uses IPv4 and IPv6 multicast since multicast MPLS is not a supported feature for Cisco ASR 1000 Series Router.

- CSCtb12998

  Not all calls are successful after RP switchover and **shutdown**, **no shutdown** of ingress interface.

  Workaround: You must reconfigure Session Border Control (SBC).

- CSCtb13472

  Label Distribution Protocol (LDP) session flaps between PE and P routers. There are 100 LDP targeted sessions between the PEs. When the targeted sessions flap, the link session between PE and P routers also flaps.

  Workaround: None

- CSCtb15399

  After prepaid (or possibly any service) download fails, the Cisco ASR 1000 Series Router crashes.

  Workaround: None

- CSCtb20400

  The Cisco ASR 1000 Series Router may crash when certain IPv6 crypto configurations are unconfigured when configurations are copied from the tftp to running config (**copy tftp: running-config**). The problem is not seen when the actual CLI is used (as opposed to **copy tftp: running-config**) on the router to unconfigure IPv6 IPsec. The problem also seems to be specific to RP2 since only the RP2 router has crashed so far, and it does not seem to affect RP1.

  Workaround: Use the CLI to unconfigure instead of configuring via the **copy tftp: running-config** command.

- CSCtb21280

  If billing is enabled with multiple instances as part of the Session Border Control (SBC) configuration, calls are processed by both instances for a short period of time and then an unexpected system reload occurs. This issue arises if billing records are being processed by a more than one billing instance.

Billing records are processed for both instances for a short time before an unexpected system reload occurs.

Workaround: At this time, using multiple billing instances leads to an unexpected system reload. Only a single billing instance can be used.

- CSCtb24845

  RADIUS throttling does not occur with a second server when there is a failover to the second server. Throttling happens for the first directed server but when there is a failover, the throttling does not happen.

  Workaround: None

- CSCtb27628

  A memory leak was observed when clearing crypto on a Cisco ASR 1000 Series Router.

  Workaround: None

- CSCtb28856

  On a Cisco ASR 1000 Series Router, in rare instances, with IP header compression (IPHC) configured, the Embedded Systems Processor (ESP) may unexpectedly reload.

  The reload of the ESP may occur when there is a high rate of traffic over an interface that is configured with IPHC and the number of configured IPHC compression-connections is lower than the number of actual flows/connections in the traffic stream.

  Workaround: Increasing the number of compression-connections will reduce the likelihood of the Embedded Systems Processor unexpectedly reloading.

- CSCtb29094

  With an ASR1002 uSBC with software redundancy, hitting no activate on billing for the second time will result in a system hang. The conditions under which this issue occurs are as follows:

  1. On a freshly rebooted router with SBC configuration
  2. Voice calls with CDR caching enabled bring down the radius server interface.

  Workaround: Don't do no activate again after the first no activate.

- CSCtb29156

  When the RADIUS remote Customer template is used on an MLNS router, MLNS brings up a session without VRF configuration. The PPPoX session is up and gets an IP address from the designated VPN Routing and Forwarding (VRF) pool.

  Workaround: Use the local Customer template and virtual private dialup network (VPDN) configuration.

- CSCtb30072

  With a 1K DMVPN spoke, if you un/re-configure tunnel protection several times and un/re-configure tunnel interface may reset both Embedded Services Processors (ESPs).

  Workaround: After unconfiguring a tunnel interface with 1K DMVPN spoke, wait for a few seconds before reconfiguring the same tunnel interface with same DMVPN configuration.

- CSCtb31090

  The active ESP resets after the active RP Switchover happens. This occurred with a scaled configuration of static virtual tunnel interfaces (VTIs) up to 2k and bi-directional traffic of throughput 3Gig. After the active RP Switchover and the new RP begins stabilizing, the active ESP resets.

  Workaround: None

- CSCtb31378

  Under certain circumstances for MPLS and multicast traffic, the forwarding plane may be unable to forward packets.

  Workaround: None

- CSCtb32037

  Traffic loss occurs during Fast Reroute (FRR) link protection in a network with 1000 TE tunnels configured for FRR during Boot up. This condition happened only when the tunnels were configured during Boot up. It did not happen when the tunnels were configured after the router was UP.

  Workaround: Configure tunnels after router has booted up.

- CSCtb32502

  With a 1K DMVPN spoke, un/re-config tunnel protection several times and un/re-config tunnel interface, RP resets.

  Workaround: Wait till all DMVPN session is up/down before next un/re-config tunnel. That is, do not un/re-configure tunnel when there are many sessions in transaction state.

- CSCtb32591

  Tunnel interfaces flap without any events as the SA's life timer expires. The tunnel goes down randomly while or when the SAs are recreated. This condition occurs with a scaled configuration of static VTIs very predominantly and with traffic (uni- or bi-directional).

  Workaround: None

- CSCtb34308

  Tracebacks are seen while initiating 4000 sessions on a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS). Tracebacks are seen when a service-policy is configured on the virtual-template and on the RADIUS profile with different names.

  Workaround: Use the same service-policy name on the Virtual-template and on the Radius profile.

- CSCtb37274

  If billing is enabled with a valid cache path as part of the SBC configuration, and records are being written to a removable device, such as a USB drive, and the device is removed from the router, an unexpected system reload can occur.

  This issue occurs if billing records are being written to a removable device and while operations are active, the device is removed from the router. Upon replacing the device and attempting to deactivate billing, an unexpected system reload occurs.

  Workaround: To avoid this issue, do not remove the device billing records are cached to while records are being processed.

- CSCtb38886

  The commands **show sbc** *name* **dbe signaling-flow stats** and **show sbc** *name* **dbe media-flow-stat** may display incorrect "Packet rate" value.

  Workaround: Ignore the "Packet rate" value in the **show** command output.

- CSCtb38954

  The issu runversion command failed on doing ISSU superpackage downgrade. On executing **issu runversion**, Switchover happened and a new active came up with the new image but then rolled back to the old image.

  Workaround: None

- CSCtb40440

  The Embedded Services Processor (ESP) may reset when applying a frame-relay map class on a channelized interface used as FR/PVC.

  Workaround: The following may cause the issue to occur:

```
interface Serial0/3/0.1/1/1/1:1
....
 frame-relay interface-dlci 16
   class <map-class-name>
```

  Use the following configuration instead of the preceding:

```
interface Serial0/3/0.1/1/1/1:1
....
 frame-relay interface-dlci 16
 frame-relay fragment 128 end-to-end
 service-policy input <service-policy-name-1>
 service-policy output <service-policy-name-2>
```

- CSCtb26955

  The following error message is displayed:

```
%CRYPTO-4-GM_REGSTER_IF_DOWN: Can't start GDOI registration as interface
FastEthernet1.2 is down
```

  However, the interface is not actually down, and so the registration should go thru. This issue occurs under the following conditions:

  1. Manually clear the rekey SA (**clear cry isakmp** *connid*)

  2) Wait for the re-registration to start.

  Workaround: Manual deleting of rekey SAs is not a valid thing to do. Using the command **clear cry gdoi** *group* or removing and adding the crytpo map works.

Resolved Caveats—Cisco IOS XE Release 2.4.1

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.4.1.

- CSCsu32069

  The Cisco ASR 1000 Series Router reloads when Call Home tries to establish a secure http connection to a server. This problem is observed under the following conditions:

  - The Call Home profile has an http destination address pointing to a secure http server.
  - No certification authority has been declared (using the **crypto pki trustpoint** command) to be used by secure http connection.

- CSCsw16157

  A Cisco ASR 1000 Series Router using Open Shortest Path First (OSPF) and Multi Protocol Label Switching Traffic Engineering (MPLS-TE) may reload or operate incorrectly following changes to the configuration of MPLS-TE tunnel interfaces or OSPF. In some instances a configuration change may cause an immediate reload. In other instances, memory may be corrupted, resulting in problems later.

- CSCsw63003

  On a Cisco ASR 1000 Series Router functioning as a provider edge (PE) router, continuous Border Gateway Protocol (BGP) activity results in the increasing allocation of BGP path attributes and increasing memory usage. Because of the continuous BGP activity, existing path attributes are not being reused, and, as a result, the number of BGP path attributes allocated increases even when the number of routes is not increasing.

- CSCsy30653

  When you delete and then re-apply a policy-map that is already attached to an interface on a Cisco ASR 1000 Series Router, the Quality of Service (QoS) classification might not take affect.

- CSCsy34917

  When a SPA is stopped before an RP switchover and then restarted after the switchover, IPSec Internet Key Exchange (IKE) packets drop and the Next Hop Resolution Protocol (NHRP) fails to come up.

- CSCsy37179

  When deleting and adding Multi Protocol Label Switching Traffic Engineering (MPLS-TE) interface tunnels on a Cisco ASR 1006 Router, the primary RP reloads and forces a switchover.

- CSCsy45414

  Open Shortest Path First version 3 (OSPFv3) sessions on a Cisco ASR 1000 Series Router flap due to the expiration of the dead timer. This condition seems to occur after a reload of the router. Executing a multicast ping does not work from one end of the link. The first hello message seems to be received, but not the subsequent ones.

- CSCsy58115

  The Border Gateway Protocol (BGP) process on a Cisco ASR 1000 Series Router may stop freeing memory and hold increased amounts of memory over time. This condition occurs because some BGP neighbors that are not in an established state are exchanging prefixes.

- CSCsy91226

  On a Cisco ASR 1000 Series Router with IP interworking in Ethernet over MPLS over GRE (EoMPLSoGRE) and keepalive enabled on a Generic Routing Encapsulation (GRE) tunnel, ip irdp packets from the customer edge (CE) router get stuck in the interface input queue of the xconnect interface.

- CSCsz31984

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when parsing certain H.225 packets by the H.323 Application Layer Gateway (ALG). This condition may be caused by malformed H.225 packets with TCP fragmentation.

- CSCsz47599

  The T3/E3 interface on a Cisco ASR 1000 Series Router does not come up after the router reloads. This condition is the result of a timing issue.

- CSCsz54781

  Session interim accounting for PPP over X (PPPoX) sessions is not functioning in Cisco IOS XE Release 2.3.0 and later releases. When interim accounting is enabled on a per-session basis, no interim accounting updates get sent to the AAA server for PPPoX sessions.

  There are no known workarounds.

- CSCsz55618

  The SSS Manager on a Cisco ASR 1000 Series Router reports a memory leak when Change of Authorization (CoA) requests are used to turn a parameterized QoS service on or off. This condition is observed when the Cisco ASR 1000 Series Router is configured with PPP Terminated Aggregation (PTA) and terminates PPPoEoQinQ sessions.

- CSCsz70244

  When either the **radius-server directed-request restricted** or **radius-server directed-request restricted** command is configured on a Cisco ASR 1000 Series Router, the authentication fails.

- CSCsz77684

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router reloads when firewall sessions are cleared using the **clear zone-pair inspect sessions** command in scaled scenarios. This condition is only associated with SIP sessions and when the SIP ALG requests many levels of sub-channels.

- CSCsz79403

  On a Cisco ASR 1000 Series Router, a Virtual Private Dialup Network (VPDN) failover does take effect with certain VPDN IP addresses. This condition occurs because two busy L2TP Network Server (LNS) IP addresses are detected. Because its busy timeout is set to 1 second, the L2TP Access Concentrator (LAC) gets stuck in a loop adding an IP address to the busy list in one second and removing the IP address from the list in the next second.

- CSCsz85306

  If Cisco Unified Border Element (SP Edition) is deactivated and activated multiple times on a Cisco ASR 1000 Series Router, an “Assertion failed” message appears on the console and the router reloads.

- CSCsz86631

  Within a few minutes of bringing up Intelligent Services Gateway (ISG) sessions and Session Border Controller (SBC) calls together on a Cisco ASR 1000 Series Router, an exception occurs and the router reloads.

- CSCsz92328

  None of the interfaces on a Cisco ASR 1000 Series Router come up after a stateful switchover (SSO) is performed on a configuration with self-signed certificates.

  This condition is observed under the following scenario:

  1. A Rivest, Shamir, and Adelman (RSA) self-signed certificate is generated on the router.

  2. The router is reloaded.

  3. An SSO is performed on the router.

- CSCsz94321

  When priority bandwidth and bandwidth remaining ratio are configured in a service-policy and the policy is enabled on an Any Transport over MPLS (AToM) virtual path (VP) on a Cisco ASR 1000 Series Router, some of the user-defined traffic classes are not guaranteed the configured bandwidth.

- CSCta01819

  Dynamically changing the session shape rate (parent shape rate) does not take effect with an IPv6 model F QoS over PPPoEoQinQ configuration on a Cisco ASR 1000 Series Router.

- CSCta04866

  When a malformed SIP message is received on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) (CUBE), traceback appears and the CUBE process reloads.

- CSCta05335

  Both the Active and Standby Route Processors (RPs) on a Cisco ASR 1000 Series Router reload during sustained traffic. This condition is observed with IPv4 calls running at 50 CPS that employ SIP INFO for Dual-Tone Multifrequency (DTMF) transport on both caller and callee.

- CSCta08805

  When a per-feature push to change the qos policy-map by a Change of Authorization (CoA) request is followed by a switchover on a Cisco ASR 1000 Series Router, the session policy-map is no longer functional after the switchover. This condition occurs because High Availability (HA) is not supported with per-feature push.

- CSCta10015

  A temporary failure to send an Internet Protocol Communications (IPC) log ACK message causes the Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router to no longer be able to receive configuration updates from the control-plane.

- CSCta11780

  Call Admission Control (CAC) and billing configurations are missing on a Cisco ASR 1000 Series Router after a double RP switchover (for example, if an RP1 to RP0 switchover is followed by an RP0 to RP1 switchover).

- CSCta11932

  On a Cisco ASR 1000 Series Router, Cisco Unified Border Element (SP Edition) only times out IPv4 end-to-end incomplete calls after it receives the media timeouts. The expected behavior is that incomplete calls will time out much sooner and at a more even rate (of 50 CPS). As a result, CUBE becomes congested. Eventually, CUBE may reach its max activating calls limit (which is 800 on an RP1), and stop accepting any new calls.

- CSCta14525

  On rare occasions, the SPA Interface Processor (SIP) card on a Cisco ASR 1000 Series Router repeatedly reloads on bootup, followed by reloads of other SIP cards and Embedded Services Processor (ESP) cards.

Open Caveats—Cisco IOS XE Release 2.4.0

This section documents possible unexpected behavior by Cisco IOS XE Release 2.4.0.

- CSCsu32069

  The Cisco ASR 1000 Series Router reloads when Call Home tries to establish a secure http connection to a server.

  This problem is observed under the following conditions:

  – The Call Home profile has an http destination address pointing to a secure http server. For example:

  ```
  destination address http
  https://172.17.46.17/its/service/oddce/services/DDCEService
  ```

  – No certification authority has been declared (using the **crypto pki trustpoint** command) to be used by secure http connection.

  Workaround: Configure a certification authority to be used by the secure http connection using the **crypto pki trustpoint** command.

- CSCsw16157

  A Cisco ASR 1000 Series Router using Open Shortest Path First (OSPF) and Multi Protocol Label Switching Traffic Engineering (MPLS-TE) may reload or operate incorrectly following changes to the configuration of MPLS-TE tunnel interfaces or OSPF. In some instances a configuration change may cause an immediate reload. In other instances, memory may be corrupted, resulting in problems later.

  To be exposed to this problem, a router must have MPLS TE tunnel interfaces that are announced to OSPF. Systems that do not run OSPF or that do not use MPLS-TE are not affected.

  Routers using MPLS-TE primary auto-tunnels are particularly vulnerable because those tunnel interfaces may be removed as a result of network topology changes as well as by modifying the running configuration.

  Routers using auto backup tunnels to provide fast reroute for static MPLS-TE tunnels do not have any extra exposure to this problem because while these backup tunnels may be removed due to topology changes, the static tunnel to the same destination will not be removed.

  Some of the configuration changes that may cause the incorrect behavior are as follows:

  – The router may reload when the following configuration commands are issued:

    Global configuration mode commands:

    * **no interface tunnel** *n*

    * **no router ospf**

    * **no mpls traffic-eng auto-tunnel**

    Interface configuration mode commands:

    * **no ip unnumbered**

    * **no ip address**

    Exec mode command:

    * **clear mpls traffic-eng auto-tunne**l

  – Removing the last MPLS-TE tunnel interface to a destination.

  - Removing an auto-tunnel configuration.
  - Removal of dynamically created auto-tunnel interfaces as a result of changes in the network topology.

  Normal UP/DOWN state changes of tunnel interfaces do not cause problems.

  Workarounds: The possible workarounds include:

  - To remove an MPLS-TE tunnel interface, first configure it down with the **shutdown** command in interface submode.
  - To remove an OSPF instance, first disable MPLS-TE for the instance by configuring the **no mpls traffic-eng area** *n* command in router ospf submode.
  - No workaround is available for MPLS-TE auto-tunnels.

- CSCsw63003 confirm as still showing Resolved

  On a Cisco ASR 1000 Series Router functioning as a provider edge (PE) router, continuous Border Gateway Protocol (BGP) activity results in the increasing allocation of BGP path attributes and increasing memory usage.

  Because of the continuous BGP activity, existing path attributes are not being reused, and, as a result, the number of BGP path attributes allocated increases even when the number of routes is not increasing.

  Workaround: Reload the router if low memory conditions are reached, or identify the root cause of the continuous activity and attempt to fix that cause if possible.

- CSCsx08861

  When an Any Transport over MPLS (AToM) virtual circuit (VC) subinterface is removed and then recreated (reprovisioned) on a Cisco ASR 1000 Series Router, the VC status on the standby RP should show as "HOTSTANDBY," but it shows as "DOWN." If a forced switchover is executed using the **redundancy force-switchover** command, the VC experiences about 44 seconds of traffic loss.

  Workaround: There are two possible workarounds for this issue.

  1. Do not reconfigure the AToM VC immediately after deleting the subinterface.
  2. Do not copy and paste the AToM VC configuration. Either do it manually step by step or copy the configuration from file.

- CSCsy19417

  When the number of Border Gateway Protocol (BGP) prefixes exceeds 300K in a Layer 3 VPN (L3VPN) scenario on a Cisco ASR 1000 Series Router and a reload is executed, Cisco Express Forwarding (CEF) is disabled. Before the reload, CEF functioned even though there were as many as 400K prefixes

  There are no known workarounds.

- CSCsy30653

  When you delete and then re-apply a policy-map that is already attached to an interface on a Cisco ASR 1000 Series Router, the Quality of Service (QoS) classification might not take affect.

  Workaround: Use a different policy-map name with the same QoS configuration.

- CSCsy34917

  When a SPA is stopped before an RP switchover and then restarted after the switchover, IPSec Internet Key Exchange (IKE) packets drop and the Next Hop Resolution Protocol (NHRP) fails to come up.

  There are no known workarounds.

- CSCsy37179

  When deleting and adding Multi Protocol Label Switching Traffic Engineering (MPLS-TE) interface tunnels on a Cisco ASR 1006 Router, the primary RP reloads and forces a switchover.

  For example:

```
interface Tunnel101
 ip unnumbered Loopback0
 ip ospf cost 65000
 tunnel destination 100.17.5.4
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng forwarding-adjacency
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth 2
 tunnel mpls traffic-eng path-option 1 explicit name PATH1
 tunnel mpls traffic-eng path-option 2 explicit name PATH2
 tunnel mpls traffic-eng path-option 3 dynamic
```

  This condition is observed after two to six delete/add cycles.

  Workaround: Limit the number of mass edits of tunnel interfaces.

- CSCsy45414

  Open Shortest Path First version 3 (OSPFv3) sessions on a Cisco ASR 1000 Series Router flap due to the expiration of the dead timer.

  This condition seems to occur after a reload of the router.

  Workaround: Perform a **shut /no shut** of the interface or a reload of the router. If you remove and add the OSPFv3 configuration on the interface, you can temporarily avoid this condition.

  Further Problem Description: Executing a multicast ping does not work from one end of the link. The first hello message seems to be received, but not the subsequent ones.

- CSCsy49927

  The IOSd process restarts and returns the following error message:

```
%Error opening tftp://202.153.144.25/hprem/rtr_crest.exp (Timed out)
```

  There are no known workarounds.

- CSCsy58115 onfirm as still showing Resolved

  The Border Gateway Protocol (BGP) process on a Cisco ASR 1000 Series Router may stop freeing memory and hold increased amounts of memory over time.

  This condition occurs because some BGP neighbors that are not in an established state are exchanging prefixes. The condition can be diagnosed by examining the out put of the **show process memory sort**, **show ip bgp sum**, and **show ip bgp vpnv4 all sum** commands. The output will show that the number of BGP attributes is increasing over time in relation to the BGP prefixes even though the number of paths remains approximately the same.

  Workaround: Remove the configurations related to the inactive neighbors (neighbors in the Idle or Active states.)

- CSCsy73014

  On a Cisco ASR 1000 Series Router, the Internet Protocol Communications (IPC) RX flow control signals do not function properly. Traffic in excess of the IPC RX rising threshold will trigger the IPC RX STOP signal. However, when traffic levels drop below the falling threshold, the IPC RX START signal will not be sent.

  There are no known workarounds.

- CSCsy91226

  On a Cisco ASR 1000 Series Router with IP interworking in Ethernet over MPLS over GRE (EoMPLSoGRE) and keepalive enabled on a Generic Routing Encapsulation (GRE) tunnel, ip irdp packets from the customer edge (CE) router get stuck in the interface input queue of the xconnect interface.

  There are no known workarounds.

- CSCsz01980

  Under very rare conditions, an RP1 on a Cisco ASR 1000 Series Router may experience an unexpected watchdog timeout during boot or shutdown and reload.

  There are no known workarounds. Following the reload, the RP1 works as expected.

- CSCsz18138

  Removing IPv4 or IPv6 addresses from VRF interfaces on a Cisco ASR 1000 Series Router results in traceback.

  There are no known workarounds.

- CSCsz23927

  When you configure both multicast sessions and Intelligent Services Gateway (ISG) sessions on a Cisco ASR 1000 Series Router, the router reloads and reports SYS-3-CPUHOG.

  Workaround: Do not configure streams with the destination address 224.1.1.44 (the multicast address.)

- CSCsz24683

  Shutting down subinterfaces configured with bidirectional forwarding detection (BFD) results in traceback.

  There are no known workarounds.

- CSCsz24818

  When the **ip telnet source interface** command is configured to point at an interface that has an IPv6 address on a Cisco ASR 1000 Series Router, the RP resets.

  Workaround: Do not use the **ip telnet source interface** command.

- CSCsz25573

  When the pado delay parameter is configured under 4000 bba-groups on a Cisco ASR 1000 Series Router configured as an L2TP Access Concentrator (LAC), the following error message appears repeatedly at the router:

  ```
  %AAA-3-ACCT_LOW_MEM_UID_FAIL: AAA unable to create UID for incoming calls due to
  insufficient
  ```

  If the configuration is saved to NVRAM, the router reloads repeatedly after a reboot

  Workaround: If the pado delay configuration is only applied to 1000 bba-groups, the problem does not occur.

- CSCsz26610

  An unexpected system reload occurs when the **crypto pki authenticate CA** command is configured on a Cisco ASR 1000 Series Router with a certificate that is missing keyUsage = cRLSign.

  Workaround: Configure the **crypto pki authenticate CA** command with a certificate that includes keyUsage = cRLSign.

- CSCsz27068

  Under rare conditions, Open Shortest Path First (OSPF) may reset when the interfaces on a Cisco ASR 1000 Series Router are unconfigured in a very short interval.

  This condition is caused by a timing issue in OSPF.

  There are no known workarounds.

- CSCsz27200

  Although the **show ip route** *ip-address* command is supported, the *ip-address* (or A.B.C.D.) option and its related parameters do not appear in the auto-completion list when the "?" or help prompt is entered for the **show ip route** command on a Cisco ASR 1000 Series Router.

  For example, note that the *ip-address* option does not appear in the list of subcommands below:

```
Router# show ip route ?
  bgp             Border Gateway Protocol (BGP)
  connected       Connected
  dhcp            Show routes added by DHCP Server or Relay
  eigrp           Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis            ISO IS-IS
  list            IP Access list
  loops           RIB routes forming loops
  mobile          Mobile routes
  multicast       Multicast global information
  odr             On Demand stub Routes
  ospf            Open Shortest Path First (OSPF)
  profile         IP routing table profile
  rip             Routing Information Protocol (RIP)
  static          Static routes
  summary         Summary of all routes
  supernets-only  Show supernet entries only
  topology        Display routes from a topology instance
  track-table     Tracked static table
  vrf             Display routes from a VPN Routing/Forwarding instance
  |               Output modifiers
```

  In addition, no list of optional parameters appear if the "?" or help prompt is entered following the **show ip route** *ip-address* command as shown below:

```
Router# show ip route 3.3.3.3 ?
% Unrecognized command
```

  But the **show ip route** *ip-address* command is supported and works as expected:

```
Router# show ip route 3.3.3.3
Routing entry for 3.3.3.3/32
  Known via "ospf 1", distance 110, metric 2, type intra area
  Last update from 63.0.0.3 on GigabitEthernet0/3/2, 4d01h ago
  Routing Descriptor Blocks:
    63.0.0.3, from 3.3.3.3, 4d01h ago, via GigabitEthernet0/3/2
      Route metric is 2, traffic share count is 1
  * 36.0.0.3, from 3.3.3.3, 4d01h ago, via GigabitEthernet0/3/0
      Route metric is 2, traffic share count is 1
Router# show ip route 3.3.3.3 | in ospf
  Known via "ospf 1", distance 110, metric 2, type intra area
```

  Workaround: The **show ip route** *ip-address* command actually is supported; its syntax just does not appear at the "?" or help prompt. For detailed information on the syntax for the **show ip route** *ip-address* command, see the following online documentation at Cisco.com:

  http://www.cisco.com/en/US/partner/docs/ios/iproute/command/reference/irp_pi2.html#wp1015483

- CSCsz31984

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when parsing certain H.225 packets by the H.323 Application Layer Gateway (ALG).

  This condition may be caused by malformed H.225 packets with TCP fragmentation.

  There are no known workarounds.

- CSCsz35479

  The Embedded Services Processor (ESP) reloads on a Cisco ASR 1000 Series Router when **shut/no shut** or soft online insertion and removal (OIR) is executed on an asynchronous transfer mode (ATM) interface that has Quality of Service (QoS) configured.

  This condition occurs when traffic is passing through the ATM interfaces at the time the **shut/no shut** sequence (or soft OIR) is performed.

  There are no known workarounds.

- CSCsz47599

  The T3/E3 interface on a Cisco ASR 1000 Series Router does not come up after the router reloads.

  This condition is the result of a timing issue.

  Workaround: Execute a **shut/no shut** on the affected interface to bring the interface up.

- CSCsz54781

  Session interim accounting for PPP over X (PPPoX) sessions is not functioning in Cisco IOS XE Release 2.3.0 and later releases. When interim accounting is enabled on a per-session basis, no interim accounting updates get sent to the AAA server for PPPoX sessions.

  There are no known workarounds.

- CSCsz55618

  The SSS Manager on a Cisco ASR 1000 Series Router reports a memory leak when Change of Authorization (CoA) requests are used to turn a parameterized QoS service on or off.

  This condition is observed when the Cisco ASR 1000 Series Router is configured with PPP Terminated Aggregation (PTA) and terminates PPPoEoQinQ sessions.

  There are no known workarounds.

- CSCsz56462

  The default behavior of the Cisco ASR 1000 Series Router is for the Cisco Discovery Protocol (CDP) to be disabled.

  Workaround: To enable CDP, include the **cdp enable** command in the configuration.

- CSCsz68932

  If a user enters an ambiguous command in adjacency sip submode on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) then the system leaves the prompt at the parent config-sbc-sbe level.

  For example, in the following sequence the user enters the ambiguous “re” command:

```
Router(config-sbc-sbe)# adjacency sip client
Router(config-sbc-sbe-adj-sip)# re
% Ambiguous command:  "re"
```

Now if the user tries to go back into the adjacency sip submode, the following error is displayed and the mode does not change:

```
Router(config-sbc-sbe)#adjacency sip client
Failed to access SBE cli configuration. Unable to execute command.
```

Workaround: Exit the config-sbc-sbe submode to the config-sbc level. Then re-enter adjacency sip submode using the **sbe** and **adjacency sip** configuration commands as follows:

```
Router(config-sbc-sbe)# exit
Router(config-sbc)#sbe
Router(config-sbc-sbe)#adjacency sip client
Router(config-sbc-sbe-adj-sip)#
```

- CSCsz70244

  When either the **radius-server directed-request restricted** or **radius-server directed-request restricted** command is configured on a Cisco ASR 1000 Series Router, the authentication fails.

  There are no known workarounds.

- CSCsz72973

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when malformed H.323 packets are received at a high rate and an Embedded Services Processor (ESP) switchover is in progress.

  This problem is intermittent

  There are no known workarounds.

- CSCsz77684

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router reloads when firewall sessions are cleared using the **clear zone-pair inspect sessions** command in scaled scenarios.

  This condition is only associated with SIP sessions and when the SIP ALG requests many levels of sub-channels.

  Workaround: To avoid this problem before clearing firewall sessions set up access control lists (ACLs) on the interfaces where the SIP flows traverse. These ACLs should deny SIP control packets (port 5060). The sessions will time out based on the idle time configured by the firewall parameter maps.

  Further Problem Description: Firewall sessions are kept in a hierarchy. The numbers of levels in this hierarchy are limited. SIP violated this limit by requesting a hierarchy of sessions hundreds of levels deep. The firewall did not protect itself from this condition. When firewall sessions are cleared, the firewall recursively follows the hierarchy of a given session to tear down all the children and sibling sessions. Because there were hundreds of levels, the firewall exhausted the stack.

- CSCsz79403

  On a Cisco ASR 1000 Series Router, a Virtual Private Dialup Network (VPDN) failover does take effect with certain VPDN IP addresses.

  This condition occurs because two busy L2TP Network Server (LNS) IP addresses are detected. Because its busy timeout is set to 1 second, the L2TP Access Concentrator (LAC) gets stuck in a loop adding an IP address to the busy list in one second and removing the IP address from the list in the next second.

  There are no known workarounds.

- CSCsz82461

  When a **match-time** command is executed on a Cisco ASR 1000 Series Router after deactivating the Cisco Unified Border Element (SP Edition) and the corresponding call policy set, an "Assertion failed" message appears on the console and the router reloads.

  There are no known workarounds.

- CSCsz82587

  If Multi Protocol Label Switching Traffic Engineering (MPLS-TE) sessions come up or go down during online insertion and removal (OIR) on a Cisco ASR 1000 Series Router, the router may reload.

  There are no known workarounds.

- CSCsz85306

  If Cisco Unified Border Element (SP Edition) is deactivated and activated multiple times on a Cisco ASR 1000 Series Router, an "Assertion failed" message appears on the console and the router reloads.

  There are no known workarounds.

- CSCsz86631

  Within a few minutes of bringing up Intelligent Services Gateway (ISG) sessions and Session Border Controller (SBC) calls together on a Cisco ASR 1000 Series Router, an exception occurs and the router reloads.

  There are no known workarounds.

- CSCsz89484

  Blacklisting of a VPN does not take effect on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) for the following configuration:

  ```
  sbe
   blacklist vpn vpn-name
    reaason authentication-failure
     trigger-size 2
  ```

  The intended blacklisting action does NOT take effect because the trigger-period is NOT configured.

  Workaround: Configure the trigger-period using the **trigger-period** *num time-units* command.

- CSCsz92328

  None of the interfaces on a Cisco ASR 1000 Series Router come up after a stateful switchover (SSO) is performed on a configuration with self-signed certificates.

  This condition is observed under the following scenario:

  1. A Rivest, Shamir, and Adelman (RSA) self-signed certificate is generated on the router.

  2. The router is reloaded.

  3. An SSO is performed on the router.

  Workaround: After the reload, remove and add the self-signed certificate.

- CSCsz94321

  When priority bandwidth and bandwidth remaining ratio are configured in a service-policy and the policy is enabled on an Any Transport over MPLS (AToM) virtual path (VP) on a Cisco ASR 1000 Series Router, some of the user-defined traffic classes are not guaranteed the configured bandwidth.

  There are no known workarounds.

- CSCsz94376

  When a very large number of calls are being processed through Cisco Unified Border Element (SP Edition) (CUBE) on a Cisco ASR 1000 Series Router and CUBE is deactivated and activated, an exception occurs and the router reloads.

  There are no known workarounds.

- CSCta00666

  W hen the Session Border Controller (SBC) **activate** command is issued on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition), the RP reloads.

  This condition is observed with SBC calls running at 50 CPS.

  There are no known workarounds.

- CSCta01819

  Dynamically changing the session shape rate (parent shape rate) does not take effect with an IPv6 model F QoS over PPPoEoQinQ configuration on a Cisco ASR 1000 Series Router.

  Workaround: Do not change the shape rate dynamically. Remove the policy map before you the change the rate and then re-attach it with the new shape rate.

- CSCta04866

  When a malformed SIP message is received on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) (CUBE), traceback appears and the CUBE process reloads.

  Workaround: Possible workarounds include:

  1. Use of SIP ports outside the standard 5060 range can help mitigate the possibility that an attacker can send malformed messages to the correct address and port.

  2. Blacklisting may help as well.

- CSCta05335

  Both the Active and Standby Route Processors (RPs) on a Cisco ASR 1000 Series Router reload during sustained traffic.

  This condition is observed with IPv4 calls running at 50 CPS that employ SIP INFO for Dual-Tone Multifrequency (DTMF) transport on both caller and callee.

  Workaround: Employ another means of DTMF transport such as RFC-2833.

- CSCta05882

  On a Cisco ASR 1000 Series Router, the Multicast Forwarding Information Base (MFIB) is not populated with the (*,G) and (S,G) entries when the **ip pim rp-address** command is configured with an access control list value.

  There are no known workarounds.

- CSCta08805

  When a per-feature push to change the qos policy-map by a Change of Authorization (CoA) request is followed by a switchover on a Cisco ASR 1000 Series Router, the session policy-map is no longer functional after the switchover.

  This condition occurs because High Availability (HA) is not supported with per-feature push.

  Workaround: To change the qos policy-map using a CoA, the service-policy should be present in either a user-profile (downloaded at authentication) or in a service-profile (downloaded at service logon).

- CSCta10015

  A temporary failure to send an Internet Protocol Communications (IPC) log ACK message causes the Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router to no longer be able to receive configuration updates from the control-plane.

  Workaround: Reload the ESP experiencing the problem.

- CSCta10764

  The Cisco Unified Border Element (SP Edition) SIP application on a Cisco ASR 1000 Series Router is not VRF-address aware when overlapping local ip addresses are used.

  Workaround: Use non-overlapping local ip addresses.

- CSCta11780

  Call Admission Control (CAC) and billing configurations are missing on a Cisco ASR 1000 Series Router after a double RP switchover (for example, if an RP1 to RP0 switchover is followed by an RP0 to RP1 switchover).

  There are no known workarounds.

- CSCta11932

  On a Cisco ASR 1000 Series Router, Cisco Unified Border Element (SP Edition) only times out IPv4 end-to-end incomplete calls after it receives the media timeouts. The expected behavior is that incomplete calls will time out much sooner and at a more even rate (of 50 CPS). As a result, CUBE becomes congested. Eventually, CUBE may reach its max activating calls limit (which is 800 on an RP1), and stop accepting any new calls.

  There are no known workarounds.

- CSCta12512

  Packets fail to get classified when the IPSec **qos-preclassify** command is configured on a Cisco ASR 1000 Series Router.

  Workaround: Re-apply the configuration, and the classification should take effect.

- CSCta14525

  On rare occasions, the SPA Interface Processor (SIP) card on a Cisco ASR 1000 Series Router repeatedly reloads on bootup, followed by reloads of other SIP cards and Embedded Services Processor (ESP) cards.

  Workaround: There are no known workarounds. The only means of recovery is to reload the router.

  Further Problem Description: The core file indicates the reload occurred in the emd (environmental monitoring) process.

Release 2.3 Caveats

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

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

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

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

This section consists of the following subsections:

Open Caveats—Cisco IOS XE Release 2.3.2

This section documents possible unexpected behavior by Cisco IOS XE Release 2.3.2

- CSCsx21652

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

  Workaround: There is no known workaround.

- CSCsy16757

  When two Cisco ASR 1000 Series Routers are set up in back-to-back mode with one router configured with a static crypto map and the other with a dynamic crypto map, the router configured with the dynamic crypto map shows outbound security associations (SAs) in the pending state for unsuccessful session set-ups.

  Workaround: Ensure that configuration on both routers is correct.

  Further Problem Description: Because pending state SAs never get deleted, eventually all SAs may be used.

- CSCsy85000

  The functionality of the standby console differs based on which Route Processor (RP) is active on a Cisco ASR 1000 Series Router. If RP0 is active and RP1 is the standby, the standby console has to be enabled manually. However, if RP1 is active and RP0 is the standby, the standby console is already enabled. The functionality should be the same regardless of which RP is active and which is the standby.

  There are no known workarounds.

- 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.

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.

  Further Problem Description: The management interface on a Cisco ASR 1000 Series Router cannot be used as an exporter source; this configuration is not supported.

- 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.

  There are no known workarounds.

- CSCsz02478

  The virtual-access interface is not re-used after a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsz46334

  In a test run of over 41 hours—sessions and TC's are constantly churned, whereby 20% of 7.5 users perform successful acct-logon and 80% of the users receive an authorization timeout. Over the duration of this test in a session-churn scenario, a RP memory leak is observed.

  Workaround: There is no known workaround.

- CSCsz47689

  During Embedded Services Processor Stateful Switchover, it takes 1200 milliseconds before the new IPv4 VoIP call can be established. The ESP-Switchover notification takes about 1 second to reach the Standby-ESP.

- CSCsz48605

  Momentary SLOS after SSO on ATM SPA interface. Conditions are: 1) ATM OC3 SPA with interface in “link / protocol down” state. 2) SSO.

  Workaround: There is no known workaround.

  Further Problem Description: This issue happens momentarily only when interfaces are in down state and SSO is performed. SLOS will come up after that; all spurious alarms will be cleared.

- CSCsz48914

  NHRP registration and tunnels are not up between the first and second level hubs. It is observed in hierarchial topology most of the time. When Cisco ASR 1000 Series Router acts as first and second level hubs, it is observed that NHRP is flapping between them and no NHRP registration is successful. This results in DMVPN network not being up.

  Workaround: There is no known workaround.

- CSCsz49249

  Embedded Services Processor (ESP) reloads when router gets invalid (wrong) ACL attribute from RADIUS server.

Workaround: There is no known workaround.

- CSCsz54781

  On enabling interim accounting on a per-session basis, no Interim accounting updates are sent to the AAA server for PPPoX sessions.

  Workaround: There is no known workaround.

- CSCsz72070

  Upgrading QoS from Mod3 to Mod4 failed in some cases.

  Workaround: There is no known workaround.

- CSCsz82080

  Under a scaled configuration (for example, 1500 DVTI remote access sessions), when all 1500 DVTI sessions are brought up at the same time in the DVTI server, the Embedded Services Processor (ESP) may reload. The problem may occur when 1500 DVTI sessions are brought up simultaneously.

  Workaround: Bring up approximately 100 Virtual Access interfaces at one time

- CSCsz90376

  The Embedded Services Processor (ESP) on the Cisco ASR 1000 Series Router may fail after a route-map is deleted and immediately added back. This may happen when a route-map configuration used in NAT translation configuration is deleted and immediately added back.

  Workaround: Add the route-map used by NAT translation back after the previous deletion is fully completed.

- CSCta15550

  Pings to a Multicast address fail, when the Cisco ASR 1000 Series Router is configured as IPSec GETVPN group member that is registered to a Key server. Multicast traffic has to pass through the group members.

  Workaround: 1) “Shutdown” followed by “no shutdown” on the group member interface which has the gdoi crypto map. 2) Execute the **clear crypto gdoi** command.

- CSCta24676

  When an attempt is made to log in to the Kerberos client, the RP fails. After the clocks of the UUTs are synchronized and the routers are configured with kerberos credentials.

  Workaround: There are no known workarounds.

- CSCta27374

  On the ASR 1000 Series Router, the update rate for statistics given by the **show policy map** command is much greater than in prior releases. The update rate has been observed to be up to 80 seconds between updates with highly scaled configurations. Note that QoS is applied on a highly scaled configuration, for example, 16K VLANs.

  Workaround: There are no known workarounds.

- CSCta38072

  Cisco IOS XE may fail while attempting to do a “redundancy force-switchover.” This is an intermittent issue.

  During a “redundancy force switchover,” the switchover occurs, but when standby bay 0 is restarting, Cisco IOS XE fails. Cisco IOS XE in standby bay 0 then restarts and the system reaches SSO.

  Workaround: There are no known workarounds.

- CSCta40724

  The reassembly router experiences a performance degradation when QoS is applied to the far end egress interface of the fragmenting router. This issue was observed when 1500 byte traffic was sent between the two routers. Without Qos applied in the fragmenting router, the performance was 750 Mbps. With Qos applied, the performance dropped to 400 Mbps.

  Conditions: Applying Qos to the egress interface can trigger this condition on traffic that is fragmented.

  Workaround: If a priority queue can be applied on the fragmenting traffic with QoS, then the result is a performance of 700 Mbps. If no priority queue can be applied, then there is no workaround.

- CSCta50363

  This condition only occurs when a large number of pinholes, for example 1440 pinholes, subscribing to NT/QUALERT have stopped receiving traffic simultaneously. The pause only occurs after a majority of notifications have been sent through. After a 5-7 minute pause, the remaining notifications come through. In this case approximately 10-15 notifications come in late.

  Workaround: There are no known workarounds.

  Further Problem Description: This issue only occurs in the rare case that traffic is stopped on a large number of pinholes simultanesouly. The effects are not considered serious. A few pinholes may report NT/QUALERT late. The loss of synchronization for the few affected pinholes is temporary and it should not affect the availability of Cisco Unified Border Element (SP Edition) services.

- CSCta55610

  The standby processor keeps on rebooting and does not come up, after a “hw-module slot R1 reload” and ISSU downgrade. The active RP is running the prior software and the standby RP is trying to come up with the downgraded software. Error message observed is: %RF-3-NOTIF_TMO: Notification timer Expired for RF Client: Redundancy Mode RF(29)

  Workaround: There are no known workarounds.

- CSCta58849

  When reloading the router, the following error message/traceback is observed: %SCHED-7-WATCH: Attempt to set uninitialized watched boolean. This is a timing issue and should only be observed if BGP is receiving data. The impact of the traceback is minimal.

  Workaround: Performing the **no router bgp** ... command before issuing the **reload** command may avoid this traceback.

  Further Problem Description: This should have minimal impact on the router, as this is a timing issue when BGP has already shut down, but before the router has reloaded. There should be no impact to routing other than what is caused by a reload.

- CSCta61656

  The **show memory debug leaks chunks** command displays 204 bytes of extended ACL leak with basic configuration. During system initialization, there is a one time allocation of a 204 byte chunk of memory that was not freed.

  Workaround: There are no known workarounds.

- CSCta65165

  Cisco IOS XE suffers a failure while executing the **show ip ospf interface** command.

  This issue occurs under the following conditions: When the Cisco ASR 1002 Router is used as an LNS. All Virtual-Access IFs are registered as OSPF Interface. And you execute the **show ip ospf interface** command when disconnecting 1000 sessions of L2TP.

Workaround: Remove the unnumbered interface of the Virtual-Template from OSPF.

- CSCta79229

  When the route map configuration is changed on PBR configured on Virtual Template with traffic running, it may cause tracebacks on the Cisco ASR 1000 Series Router; eventually the system recovers.

  Further Problem Description: Changing the route map on the fly involves removal of route map information from the data path and addition of new route map information in the data path. Because traffic is continuously running, some lookups may fail and cause temporary error conditions.

  Workaround: There are no known workarounds.

- CSCta93930

  The Embedded Services Processor (ESP) eventually suffers a major failure after about 800,000 PPP sessions flap with the IP virtual-reassembly feature configured, either through the virtual-template or RADIUS. This problem is preceded by a %CPPDRV-4-ADRSPC_LIMIT log message.

  Conditions are: The IP virtual-reassembly feature must be configured on the virtual-template or RADIUS. PPP sessions using this feature must flap. This problem may occur on PTA sessions as well as LNS. This problem was observed on ESP20 and may occur on ESP10 as well.

  Workaround: Disable the IP virtual-reassembly feature or limit its deployment to PPP subscribers who need it. Monitor for %CPPDRV-4-ADRSPC_LIMIT log messages.

- CSCta94710

  Cisco ASR 1000 Series Route Processor (RP) fails. This problem occurs under the following conditions:

  1. You have a Cisco ASR 1000 Series Route Processor 2 (RP2).

  2. You have defined a VRF and configured it under any interface (physical/tunnel).

  3. You have disabled split horizon at interface level.

  4. You have configured EIGRP routing protocol.

  5. You advertise the network through the **address family ipv4 vrf** command.

  Workaround: Do not disable split horizon.

- CSCta99173

  The Embedded Services Processor 20 (ESP20) may core dump and reload following the churning of approximately 880,000 PPP sessions with firewall and ip virtual-reassembly features configured on those PPP sessions.

  This problem does not occur with PPP sessions that do not have VFR configured.

  This problem occurs under the following conditions: The PPP sessions must have firewall configured (have a zone configured as part of a zone-pair policy) and have ip virtual-reassembly (virtual fragmentation reassembly and VFR) configured.

  Workaround: Remove the VFR feature from the PPP sessions.

- CSCta99654

  (S,G) entry does not have the translated entry with NAT outside static/dynamic configured.

  With multicast and NAT outside static/dynamic configured, translated packets are not punted to the Route Processor (RP). The (S,G) entry on the UUT has the pre-NAT entry instead of the translated entry.

  Workaround: There is no known workaround.

Resolved Caveats—Cisco IOS XE Release 2.3.2

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.3.2.

- CSCsy05298

  When a large number of groups (for example, 50) is configured on a Cisco ASR 1000 Series Router and the **show crypto gdoi** command is issued, the IOSD process reloads.

  This condition occurs after the general configuration is applied and after the ping is checked between all the Protocol Independent Multicast (PIM) neighbors.

  Workaround: Use the **show crypto gdoi group** *group-name* command to display information for a specific group.

- CSCsy15018

  After the **show ip cache flow** command is executed 4 to 5 times on a Cisco ASR 1000 Series Router configured with NetFlow, the command returns false counters for the Total field. These false counters are only observed for a few seconds.

  This condition occurs when e**nable in/e gress netflow** is configured on 2 to 3 subinterfaces with **set term len** equal to 20.

  There are no known workarounds.

- CSCsy17832

  In rare instances, Layer 2 Tunnel Protocol (L2TP) tunnels/sessions are lost after a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsy41352

  The Cisco ASR 1000 Series Router does not generate an Internet Control Management Protocol (ICMP) redirect message over Generic Routing Encapsulation (GRE) tunnels.

  This condition occurs when there is an egress route pointing to the same GRE tunnel over which the packet came into the router.

  There are no known workarounds.

- CSCsy45907

  If the **show sbc global dbe media-stats** command is issued while the data border element (DBE) is being deleted on a Cisco ASR 1000 Series Router, the active Route Processor reloads.

  There are no known workarounds.

- CSCsy54486

  When an Internet Control Management Protocol (ICMP) Router Solicitation message is send from a source address of 0.0.0.0, the Cisco ASR 1000 Series Router drops the packet.

  There are no known workarounds.

- CSCsy58924

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reset if a certain combination of deny access control entries (ACEs) are added to a Web Cache Communication Protocol (WCCP) access control list (ACL).

  Workaround: Shut down the interface to the Wide Area Application Engine (WAE).

Further Problem Description: This problem can occur in the broadband remote access server (BRAS) scenario also and is related to the size of certain Internet Protocol Communications (IPC) messages.

- CSCsy60103

  The Cisco ASR 1000 Series Router reports a cmand crash during a router reload.

  Workaround: The router should function normally after the reload. No workaround is necessary.

- CSCsy70911

  When the source of the exporter is set to the management interface, the source displays as unknown in the output of the **show ip flow export** command.

  Workaround: Do not assign the management interface as the source of the exporter.

- CSCsy74452

  A Cisco ASR 1000 Series Router running Cisco IOS XE Release 2.3.0 cannot download an ip access-list configuration with multiple port numbers in one access control entry (ACE) to the Cisco QuantumFlow Processor.

  This error is observed if a user configures an ip access-list with more than one port number after the **eq** or **neq** keywords.

  For example:

```
Router(config)#ip access-list ext testxxx
Router(config-ext-nacl)#permit tcp any any eq 2001 2002 2003
Router(config-ext-nacl)# *Mar 28 05:34:51.576: %FMFP_ACL-3-ACL_OBJECT_DOWNLOAD: F0:
fman_fp_image: ACL actions for ACL testxxx fail to download because Bad address.
*Mar 28 05:34:51.577: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image: ACL 14
download to CPP failed
```

  Workaround: Put only one port number after **eq** or **neq** keywords. The following are examples of specific workarounds:

  Example 1

  Convert one ACE configuration with multiple **eq** ports to multiple ACEs with one port as follows:

  Change the ACE from:

```
permit tcp any any eq 2001 2002 2003
```

  to:

```
permit tcp any any eq 2001
permit tcp any any eq 2002
permit tcp any any eq 2003
```

  Example 2

  Convert one ACE configuration with multiple **neq** values to multiple separate ranges as follows:

  Change the ACE from:

```
permit tcp any any neq 2001 3001
```

  to:

```
permit tcp any any lt 2001
permit tcp any any range 2002 3000
permit tcp any any gt 3001
```

Example 3

Convert one ACE configuration with multiple values for both the source and destination port to multiple combinations as follows:

Change the ACE from:

```
permit tcp any eq 2001 2002 any eq 3001 3002
```

to:

```
permit tcp any eq 2001 any eq 3001
permit tcp any eq 2001 any eq 3002
permit tcp any eq 2002 any eq 3001
permit tcp any eq 2002 any eq 3002
```

- CSCsy77269

  The Cisco ASR 1000 Series Router reloads when executing a s**how crypto ipsec sa identity** command.

  This condition seems to occur while Group Encrypted Transport VPN (GET VPN) is doing a rekey.

  Workaround: Wait for the GET VPN rekey to finish before executing a **show crypto ipsec sa identity** command. You can also increase the lifetime of the security associations (SAs) so that rekeys happen less frequently.

- CSCsy78488

  One or more of the following symptoms can be seen on a Cisco ASR 1000 Series Router:

  – The **show platform hardware cpp active feature fnf datapath all** and s**how ip cache flow** commands might not work for following aggregation caches:

    - Destination prefix aggregation (destination mask only)

    - Destination prefix TOS aggregation (destination mask only)

    - Prefix aggregation (source and destination mask)

    - Prefix-port aggregation (source and destination mask)

    - Prefix-TOS aggregation (source and destination mask)

    - Source prefix aggregation (source mask only)

    - Source prefix TOS aggregation (source mask only)

  – Denies associating the egress and ingress monitors with the caches.

  – Resource (memory) leakage

  These conditions may occur when the following configuration is configured under the **ip flow-aggregation cache** *cache-type* command sub-mode for the above mentioned cache types:

  mask {[**destination** | **source**] **minimum** *value*

  Workaround: Do not configure **mask** {[**destination** | **source**] **minimum** *value*} for the caches described in the first bullet.

  Further Problem Description: With the workaround a mask value of 0 is used as the default. As a result, NetFlow collection granularity will be coarse.

- CSCsy81461

  If a GM is left for re-keying for a long interval, NO IPSEC FLOWS messages display on the Cisco ASR 1000 Series Router console and the IPSec security association (SA) download fails.

  There are no known workarounds.

- CSCsy83163

  On a Cisco ASR 1000 Series Router, a Secure Shell (SSH) session on a Telnet connection hangs as soon as AAA Authentication is successful and the target router's prompt is received.

  Workaround: Do not attempt an SSH connection from within a Telnet session.

- CSCsy83413

  When 1k Dynamic Multipoint VPN (DMVPN) IPSec tunnels are established with a hub-spoke topology on a Cisco ASR 1000 Series Router, a memory leak occurs at the “eventutil” module.

  There are no known workarounds.

- CSCsy92358

  The IOSD process on a Cisco ASR 1000 Series Router may run out of memory if left running with an IPSec and Multipoint GRE (mGRE) configuration for long intervals.

  There are no known workarounds.

  Further Problem Description: The router may eventually reload due to an invalid handling of memory allocation failure.

- CSCsy93931

  The Cisco ASR 1000 Series Router does not reset the timeout value down to 60 seconds upon receipt of a FIN/RST/SYN for a Transmission Control Protocol (TCP) session when the **no-payload** keyword is used on the mapping. As a result, larger than expected Network Address Translation (NAT) translation tables are observed in the output of the s**how ip nat statistics** command.

  Workaround: Remove the **no-payload** keyword, or manually reset the nat tcp timeout down to 60 seconds.

- CSCsy94554

  When the **clear ipv6 neighbor** command is issued on a Cisco ASR 1000 Series Router, the adjacency of the ipv6 next-hop will be incomplete if it is needed to resolve a 6to4 tunnel.

  Workaround: Perform the **shutdown** and **no shutdown** commands on the 6to4 tunnel.

- CSCsy95109

  Some virtual circuits remain down after an asynchronous transfer mode (ATM) SPA and SIP reload.

  This condition has been observed with 100 virtual path (VP) pseudowires (PWs).

  Workaround: Enter the **clear ospf process** command.

- CSCsy96344

  When the **clear ip nat trans *** command is executed while an overloaded configuration with extremely high scaling is running, the Cisco ASR 1000 Series Router may reload.

  There are no known workarounds.

- CSCsy96501

  Performing an in-service software upgrade (ISSU) sub-package upgrade from Cisco IOS XE Release 2.2.3 to Cisco IOS XE Release 2.3.1 results in “CPPOSLIB-3-ERROR_NOTIFY” traceback and two core files while upgrading the active Embedded Services Processor (ESP).

  There are no known workarounds.

- CSCsy96761

  Removing NetFlow from the last/only interface may cause the Embedded Services Processor (ESP) on a Cisco ASR 1000 Series ESP board to reload.

This condition is caused by a race condition between the Cisco QuantumFlow Processor ager logic verses the code that processes the ager shutdown administrative action. If the ager shutdown code executes while the periodic ager function is executing, the ager function may reuse the timer structure, which is subsequently freed as part of the ager shutdown.

Workaround: The timing window can be reduced to near 0 by taking the following steps:

1. Configure NetFlow on interface x with no traffic.
2. Deconfigure NetFlow from all other interfaces.
3. Wait for all entries in the NetFlow cache to be aged out.
4. Then deconfigure NetFlow from the inactive interface x.

- CSCsy97794

  Policy Based Routing (PBR) stops working on a Cisco ASR 1000 Series Router after **ip policy route-map** is applied on the IPSec Dynamic Virtual Tunnel Interface (DVTI) interface.

  Workaround: Save the configuration and reboot the router.

- CSCsy99103

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router reloads if a **configure replace** command is executed that results in many configuration changes.

  This condition was observed on a Cisco ASR 1004 Router running Cisco IOS XE Release 2.2.3.

  Workaround: Do use the **configure replace** command.

- CSCsz01854

  CE-to-CE communication stops after the main interface on a Cisco ASR 1000 Series Router (configured as a PE) is brought up and the Hot Standby Routing Protocol (HSRP) takes over as active on the subinterface.

  Workaround: Fail over the HSRP on the Cisco ASR 1000 Series Router to the other HSRP subinterface and then fail it back.

- CSCsz02404

  A Cisco ASR 1000 Series Router may reload when the router is configured with Network Address Translation (NAT) at extremely high dynamic bind scaling.

  There are no known workarounds.

- CSCsz04555

  A SPA-1X10GE-L-V2 on a Cisco ASR 1000 Series Router may reload when subjected to high Bit Error Rates.

  Workaround: There are no known workarounds. The module will reload and come back up. A shut/no shut should bring the interface back online.

- CSCsz05918

  Cisco Discovery Protocol (CDP) neighbors do not come up on the VLAN subinterface between two Cisco ASR 1000 Series Routers or a Cisco ASR 1000 Series Router and a Cisco 7600 Series Router or Cisco 7200 Series Router.

  This condition occurs because CDP is enabled on the VLAN subinterface but disabled on main interface.

  Workaround: Activate CDP on the main interface.

- CSCsz12276

  Dynamic Multipoint VPN (DMVPN) stops functioning if you configure a dynamic crypto map on the physical interface of a Cisco ASR 1000 Series Router running Cisco IOS XE Release 2.3.0.

  Workaround: Downgrade the software to Cisco IOS XE Release 2.2.x Cisco IOS XE Release 2.1.x.

- CSCsz18158

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may unexpectedly reload during a complex NetFlow-related reconfiguration.

  This condition is observed when a large-scale NetFlow configuration (such as many instances of NetFlow on interfaces/subinterfaces) is used in conjunction with dynamic reconfiguration. For example:

```
int range te0/2/0.2 - te0/2/0.1001
no flow-sampler abc
no flow-sampler abc eg
!
int te1/3/0
no flow-sampler abc
no flow-sampler abc eg int range te0/2/0.2 - te0/2/0.1001
flow-sampler abc
flow-sampler abc eg
!
int te1/3/0
flow-sampler abc
flow-sampler abc eg
```

  Workaround: Wait for some pending actions to complete before entering the next command.

  For example, the following command sequence shows the same sequence of commands as in the example above, but the sequence is interspersed with two wait intervals:

```
int range te0/2/0.2 - te0/2/0.1001
no flow-sampler abc
no flow-sampler abc eg
!
int te1/3/0
no flow-sampler abc
no flow-sampler abc eg
! WORKAROUND STEP
! Wait for pending actions to complete by entering the show platform soft object f0
! stat command.
! Repeat this show command until the status is "no actions pending".
int range te0/2/0.2 - te0/2/0.1001
flow-sampler abc
flow-sampler abc eg
!
int te1/3/0
flow-sampler abc
flow-sampler abc eg
! WORKAROUND STEP
! Wait for pending actions to complete by entering the show platform soft object f0
! stat command.
! Repeat this show command until the status is "no actions pending".
```

  Further Problem Description: This condition is a timing-related problem that tends to occur with a large dynamic reconfiguration. The workaround avoids the timing-related issue by enforcing atomicity between separate phases of the reconfiguration.

- CSCsz21313

  A Cisco ASR 1000 Series Router reloads with the __be_c3pl_action_account_queueing_stats_free message when removing a subscriber policy with the account feature configured from the port-channel.

  Workaround: Do not configure the account feature within a subscriber policy. The account feature is not supported in Cisco IOS XE Release 2.3.

- CSCsz21732

  A Cisco ASR 1000 Series Router may reload when configured for Simple Network Management Protocol (SNMP) inform notifications.

  Workaround: Disable inform notifications using the **no snmp-server host host-address informs** command.

- CSCsz44301

  During platform Route Processor (RP) switchover, root hub is not seeing NHRP registration messages from first level hubs. After RP swtichover, NHRP is not registered to root hub.

  Workaround: There are no known workarounds.

- CSCsz45152

  The Environment Monitoring Daemon (EMD) is a process dedicated to collection and transmission of chassis-environment statistics information such as temperature, and so forth. This process periodically transmits the information using messages.

  During the early stages of bringup (after a reload), EMD fails while attempting to create and transmit the first of one such message. This problem happens during bringup that immediately follows the router reload (using the **reload** command), with auto-boot configured. It happens in Cisco IOS XE Release 2.3.2 and earlier releases.

  Workaround: There is no workaround. EMD restarts after the failure and usually works as expected.

- CSCsz47599

  The SPA-4XT3/E3 serial interface does not come up after the router reloads. It is a timing issue and is not always seen.

  Workaround: Performing a shut and no-shut interface brings up the interface.

  Further Problem Description: Sometimes in a router reload case, if the interface state event comes earlier before the interface is registered, the event is ignored. As a workaround: perform a shut and no-shut of the interface; the system asks for another interface state event and handles bringing up the interface this time.

- CSCsz81459

  Issue 1. After Route Processor (RP) SSO on a DMVPN hub, hub locally generated packets bypass IPsec encryption on hub to spoke tunnel. The spoke will not be able process traffic generated by the hub, such as EIGRP packets. The problem is only observed when the Cisco ASR 1000 Series Router acts as a DMVPN hub and DMVPN spoke. This issue is only applicable for a Cisco ASR 1000 Series Router RP switchover.

  Workaround 1: Save the configuration and reboot the router. Preservation of IPSec sessions after SSO is not a supported feature in the release.

  Issue 2. DMVPN with IPSEC tunnel fails to come-up after SSO. This issue is DMVPN with IPSEC only and is applicable only after SSO.

  Workaround 2: Clear the adjacency.

Further Problem Description: After SSO, platform multicast adjacency is not repopulated due to race condition between tunnel-up notification and FIB repopulate request.

- CSCsz85092

  Cisco ASR 1000 Series Router fails while changing NAT configuration from Dynamic NAT to PAT with traffic on.

  Workaround: Stop the traffic and change NAT translations.

- CSCta02570

  Cisco IOS XE resets while bringing up a large number of dVTIs, in this case 1500 dVTIs, at the same time.

- CSCta04880

  This problem occurs when running EoMPLSoGREoIPSec using an IPsec protection profile on the GRE tunnel. If we unconfigure the IPsec profile from the GRE tunnel interface and it is the last IPsec tunnel configured in the router, the ESP may reload. This problem causes all traffic being forwarded by the ESP to be dropped and the Cisco ASR 1000 Series Router needs to be reloaded for services to recover.

  The problem is observed if EoMPLS over GRE tunnel traffic is being encrypted or decrypted on the Cisco ASR 1000 Series Router with ESP20 and RP1. The issue can also be seen with other types of configuration such as IPv6 IPsec SVTI configuration and EIGRP over DMVPN configuration. This problem occurs frequently under common conditions and configurations

  Workaround: Configure a dummy IPsec tunnel with no peer. Therefore, the in-use IPsec tunnel will not be the last one to be removed in the router.

- CSCta07106

  The initial packet is dropped for mcast conditions. It happens in PIM-SM and PIM-DM.

  Workaround: There is no known workaround.

- CSCta33011

  Not able to terminate PPPoE sessions on the Cisco ASR 1000 Series Router. The problem starts after days of normal working operations where the Cisco ASR 1000 Series Router is configured as an LNS.

- CSCta43602

  The MFIB code translates the packet received on the output interface to 0.0.0.0 and simply drops the packet. The PIM assert mechanism is not triggered with NAT when the original source address is the same as the translated source address.

  Workaround: There is no known workaround.

- CSCta45260

  Cisco IOS XE may fail while attempting to do IPv6 neighbor resolution. For this issue to occur, the control plane update for removing an IPv6 route must pass the in-flight request from the data-path to initiate neighbor discovery for a specific V6 address reachable by the changing route.

  Workaround: There is no known workaround.

- CSCta58499

  RP fails at the Mwheel process. This problem was observed when booting two routers at the same time or doing an RP switchover.

  Workaround: There is no known workaround.

- CSCta58589

  The cpp_cp process running on the Embedded Services Processor (ESP) fails, causing the ESP to reload. This problem is caused by a sequence of QoS configuration and interface addition/deletion changes or rate changes performed at the same time.

- CSCta58800

  An Embedded Services Processor (ESP) reset occurs and the following (or similar) error message is displayed on the system console: *Jul 8 17:53:31.674 IST: %CPPHA-3-FAULT: F0: cpp_ha: CPP:0 desc:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR(interrupt) class:OTHER sev:FATAL id:1995 cppstate:RUNNING res:UNKNOWN flags:0x7 cdmflags:0x0

  This problem may occur when a hierarchical policy-map is rapidly configured, deconfigured, and configured on a GigabitEthernet interface. The parent policy-map must have serveral child classes each referencing the same output child policy-map. The child policy-map must have random-detect configured in some of its classes.

  Workaround: After deconfiguing the policy-map, wait approximately 30 seconds before reconfiguring it.

- CSCta69720

  The route processor (RP) is observed to reload after 24 hours.

  When 10K sessions out of 23K sessions are flapped for 24 hours, the RP is observed to reload and switchover is observed.

Open Caveats—Cisco IOS XE Release 2.3.1

This section documents possible unexpected behavior by Cisco IOS XE Release 2.3.1.

- CSCsy05298

  When a large number of groups (for example, 50) is configured on a Cisco ASR 1000 Series Router and the **show crypto gdoi** command is issued, the IOSD process reloads.

  This condition occurs after the general configuration is applied and after the ping is checked between all the Protocol Independent Multicast (PIM) neighbors.

  Workaround: Use the **show crypto gdoi group** *group-name* command to display information for a specific group.

- CSCsy15018

  After the **show ip cache flow** command is executed 4 to 5 times on a Cisco ASR 1000 Series Router configured with NetFlow, the command returns false counters for the Total field. These false counters are only observed for a few seconds.

  This condition occurs when **enable in/e gress netflow i**s configured on 2 to 3 subinterfaces with **set term len** equal to 20.

  There are no known workarounds.

- CSCsy16757

  When two Cisco ASR 1000 Series Routers are set up in back-to-back mode with one router configured with a static crypto map and the other with a dynamic crypto map, the router configured with the dynamic crypto map shows outbound security associations (SAs) in the pending state for unsuccessful session set-ups.

Workaround: Ensure that configuration on both routers is correct.

Further Problem Description: Because pending state SAs never get deleted, eventually all SAs may be used.

- CSCsy17832

  In rare instances, Layer 2 Tunnel Protocol (L2TP) tunnels/sessions are lost after a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- 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.

  There are no known workarounds.

- CSCsy41352

  The Cisco ASR 1000 Series Router does not generate an Internet Control Management Protocol (ICMP) redirect message over Generic Routing Encapsulation (GRE) tunnels.

  This condition occurs when there is an egress route pointing to the same GRE tunnel over which the packet came into the router.

  There are no known workarounds.

- CSCsy45907

  If the **show sbc global dbe media-stats** command is issued while the data border element (DBE) is being deleted on a Cisco ASR 1000 Series Router, the active Route Processor reloads.

  There are no known workarounds.

- CSCsy54486

  When an Internet Control Management Protocol (ICMP) Router Solicitation message is send from a source address of 0.0.0.0, the Cisco ASR 1000 Series Router drops the packet.

  There are no known workarounds.

- CSCsy58924

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reset if a certain combination of deny access control entries (ACEs) are added to a Web Cache Communication Protocol (WCCP) access control list (ACL).

  Workaround: Shut down the interface to the Wide Area Application Engine (WAE).

  Further Problem Description: This problem can occur in the broadband remote access server (BRAS) scenario also and is related to the size of certain Internet Protocol Communications (IPC) messages.

- CSCsy60103

  The Cisco ASR 1000 Series Router reports a cmand crash during a router reload.

  Workaround: The router should function normally after the reload. No workaround is necessary.

- CSCsy70911

  When the source of the exporter is set to the management interface, the source displays as unknown in the output of the **show ip flow export** command.

  Workaround: Do not assign the management interface as the source of the exporter.

- CSCsy74452

  A Cisco ASR 1000 Series Router running Cisco IOS XE Release 2.3.0 can not download an ip access-list configuration with multiple port numbers in one access control entry (ACE) to the Cisco QuantumFlow Processor.

  This error is observed if a user configures an ip access-list with more than one port number after the **eq** or **neq** keywords.

  For example:

```
Router(config)#ip access-list ext testxxx
Router(config-ext-nacl)#permit tcp any any eq 2001 2002 2003
Router(config-ext-nacl)# *Mar 28 05:34:51.576: %FMFP_ACL-3-ACL_OBJECT_DOWNLOAD: F0:
fman_fp_image: ACL actions for ACL testxxx fail to download because Bad address.
*Mar 28 05:34:51.577: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image: ACL 14
download to CPP failed
```

  Workaround: Put only one port number after **eq** or **neq** keywords. The following are examples of specific workarounds:

  Example 1

  Convert one ACE configuration with multiple **eq** ports to multiple ACEs with one port as follows:

  Change the ACE from:

```
permit tcp any any eq 2001 2002 2003
```

  to:

```
permit tcp any any eq 2001
permit tcp any any eq 2002
permit tcp any any eq 2003
```

  Example 2

  Convert one ACE configuration with multiple **neq** values to multiple separate ranges as follows:

  Change the ACE from:

```
permit tcp any any neq 2001 3001
```

  to:

```
permit tcp any any lt 2001
permit tcp any any range 2002 3000
permit tcp any any gt 3001
```

  Example 3

  Convert one ACE configuration with multiple values for both the source and destination port to multiple combinations as follows:

  Change the ACE from:

```
permit tcp any eq 2001 2002 any eq 3001 3002
```

  to:

```
permit tcp any eq 2001 any eq 3001
permit tcp any eq 2001 any eq 3002
permit tcp any eq 2002 any eq 3001
permit tcp any eq 2002 any eq 3002
```

- CSCsy77269

  The Cisco ASR 1000 Series Router reloads when executing a s**how crypto ipsec sa identity** command.

  This condition seems to occur while Group Encrypted Transport VPN (GET VPN) is doing a rekey.

  Workaround: Wait for the GET VPN rekey to finish before executing a **show crypto ipsec sa identity** command. You can also increase the lifetime of the security associations (SAs) so that rekeys happen less frequently.

- CSCsy78488

  One or more of the following symptoms can be seen on a Cisco ASR 1000 Series Router:

  – The **show platform hardware cpp active feature fnf datapath all** and s**how ip cache flow** commands might not work for following aggregation caches:

    - Destination prefix aggregation (destination mask only)

    - Destination prefix TOS aggregation (destination mask only)

    - Prefix aggregation (source and destination mask)

    - Prefix-port aggregation (source and destination mask)

    - Prefix-TOS aggregation (source and destination mask)

    - Source prefix aggregation (source mask only)

    - Source prefix TOS aggregation (source mask only)

  – Denies associating the egress and ingress monitors with the caches.

  – Resource (memory) leakage

  These conditions may occur when the following configuration is configured under the **ip flow-aggregation cache** *cache-type* command sub-mode for the above mentioned cache types:

  mask {[**destination** | **source**] **minimum** *value*

  Workaround: Do not configure **mask** {[**destination** | **source**] **minimum** *value*} for the caches described in the first bullet.

  Further Problem Description: With the workaround a mask value of 0 is used as the default. As a result, NetFlow collection granularity will be coarse.

- CSCsy81461

  If a GM is left for re-keying for a long interval, NO IPSEC FLOWS messages display on the Cisco ASR 1000 Series Router console and the IPSec security association (SA) download fails.

  There are no known workarounds.

- CSCsy83163

  On a Cisco ASR 1000 Series Router, a Secure Shell (SSH) session on a Telnet connection hangs as soon as AAA Authentication is successful and the target router's prompt is received.

  Workaround: Do not attempt an SSH connection from within a Telnet session.

- CSCsy83413

  When 1k Dynamic Multipoint VPN (DMVPN) IPSec tunnels are established with a hub-spoke topology on a Cisco ASR 1000 Series Router, a memory leak occurs at the “eventutil” module.

  There are no known workarounds.

- CSCsy85000

  The functionality of the standby console differs based on which Route Processor (RP) is active on a Cisco ASR 1000 Series Router. If RP0 is active and RP1 is the standby, the standby console has to be enabled manually. However, if RP1 is active and RP0 is the standby, the standby console is already enabled. The functionality should be the same regardless of which RP is active and which is the standby.

  There are no known workarounds.

- 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.

  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.

  Further Problem Description: The management interface on a Cisco ASR 1000 Series Router cannot be used as an exporter source; this configuration is not supported.

- CSCsy92358

  The IOSD process on a Cisco ASR 1000 Series Router may run out of memory if left running with an IPSec and Multipoint GRE (mGRE) configuration for long intervals.

  There are no known workarounds.

  Further Problem Description: The router may eventually reload due to an invalid handling of memory allocation failure.

- CSCsy93931

  The Cisco ASR 1000 Series Router does not reset the timeout value down to 60 seconds upon receipt of a FIN/RST/SYN for a Transmission Control Protocol (TCP) session when the **no-payload** keyword is used on the mapping. As a result, larger than expected Network Address Translation (NAT) translation tables are observed in the output of the s**how ip nat statistics** command.

  Workaround: Remove the **no-payload** keyword, or manually reset the nat tcp timeout down to 60 seconds.

- CSCsy94554

  When the **clear ipv6 neighbor** command is issued on a Cisco ASR 1000 Series Router, the adjacency of the ipv6 next-hop will be incomplete if it is needed to resolve a 6to4 tunnel.

  Workaround: Perform the **shutdown** and **no shutdown** commands on the 6to4 tunnel.

- CSCsy95109

  Some virtual circuits remain down after an asynchronous transfer mode (ATM) SPA and SIP reload.

  This condition has been observed with 100 virtual path (VP) pseudowires (PWs).

  Workaround: Enter the **clear ospf process** command.

- CSCsy96344

  When the **clear ip nat trans *** command is executed while an overloaded configuration with extremely high scaling is running, the Cisco ASR 1000 Series Router may reload.

  There are no known workarounds.

- CSCsy96501

  Performing an in-service software upgrade (ISSU) sub-package upgrade from Cisco IOS XE Release 2.2.3 to Cisco IOS XE Release 2.3.1 results in "CPPOSLIB-3-ERROR_NOTIFY" traceback and two core files while upgrading the active Embedded Services Processor (ESP).

  There are no known workarounds.

- CSCsy96761

  Removing NetFlow from the last/only interface may cause the Embedded Services Processor (ESP) on a Cisco ASR 1000 Series ESP board to reload.

  This condition is caused by a race condition between the Cisco QuantumFlow Processor ager logic verses the code that processes the ager shutdown administrative action. If the ager shutdown code executes while the periodic ager function is executing, the ager function may reuse the timer structure, which is subsequently freed as part of the ager shutdown.

  Workaround: The timing window can be reduced to near 0 by taking the following steps:

  1. Configure NetFlow on interface x with no traffic.
  2. Deconfigure NetFlow from all other interfaces.
  3. Wait for all entries in the NetFlow cache to be aged out.
  4. Then deconfigure NetFlow from the inactive interface x.

- CSCsy97794

  Policy Based Routing (PBR) stops working on a Cisco ASR 1000 Series Router after **ip policy route-map** is applied on the IPSec Dynamic Virtual Tunnel Interface (DVTI) interface.

  Workaround: Save the configuration and reboot the router.

- CSCsy99103

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router reloads if a **configure replace** command is executed that results in many configuration changes.

  This condition was observed on a Cisco ASR 1004 Router running Cisco IOS XE Release 2.2.3.

  Workaround: Do use the **configure replace** command.

- CSCsz01854

  CE-to-CE communication stops after the main interface on a Cisco ASR 1000 Series Router (configured as a PE) is brought up and the Hot Standby Routing Protocol (HSRP) takes over as active on the subinterface.

  Workaround: Fail over the HSRP on the Cisco ASR 1000 Series Router to the other HSRP subinterface and then fail it back.

- CSCsz02404

  A Cisco ASR 1000 Series Router may reload when the router is configured with Network Address Translation (NAT) at extremely high dynamic bind scaling.

  There are no known workarounds.

- CSCsz02478

  The virtual-access interface is not re-used after a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsz04555

  A SPA-1X10GE-L-V2 on a Cisco ASR 1000 Series Router may reload when subjected to high Bit Error Rates.

  Workaround: There are no known workarounds. The module will reload and come back up. A shut/no shut should bring the interface back online.

- CSCsz05918

  Cisco Discovery Protocol (CDP) neighbors do not come up on the VLAN subinterface between two Cisco ASR 1000 Series Routers or a Cisco ASR 1000 Series Router and a Cisco 7600 Series Router or Cisco 7200 Series Router.

  This condition occurs because CDP is enabled on the VLAN subinterface but disabled on main interface.

  Workaround: Activate CDP on the main interface.

- CSCsz12276

  Dynamic Multipoint VPN (DMVPN) stops functioning if you configure a dynamic crypto map on the physical interface of a Cisco ASR 1000 Series Router running Cisco IOS XE Release 2.3.0.

  Workaround: Downgrade the software to Cisco IOS XE Release 2.2.x Cisco IOS XE Release 2.1.x.

- CSCsz18158

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may unexpectedly reload during a complex NetFlow-related reconfiguration.

  This condition is observed when a large-scale NetFlow configuration (such as many instances of NetFlow on interfaces/subinterfaces) is used in conjunction with dynamic reconfiguration. For example:

```
int range te0/2/0.2 - te0/2/0.1001
no flow-sampler abc
no flow-sampler abc eg
!
int te1/3/0
no flow-sampler abc
no flow-sampler abc eg int range te0/2/0.2 - te0/2/0.1001
flow-sampler abc
flow-sampler abc eg
!
int te1/3/0
flow-sampler abc
flow-sampler abc eg
```

  Workaround: Wait for some pending actions to complete before entering the next command.

  For example, the following command sequence shows the same sequence of commands as in the example above, but the sequence is interspersed with two wait intervals:

```
int range te0/2/0.2 - te0/2/0.1001
no flow-sampler abc
no flow-sampler abc eg
!
int te1/3/0
no flow-sampler abc
```

```
no flow-sampler abc eg
! WORKAROUND STEP
! Wait for pending actions to complete by entering the show platform soft object f0
! stat command.
! Repeat this show command until the status is "no actions pending".
int range te0/2/0.2 - te0/2/0.1001
flow-sampler abc
flow-sampler abc eg
!
int te1/3/0
flow-sampler abc
flow-sampler abc eg
! WORKAROUND STEP
! Wait for pending actions to complete by entering the show platform soft object f0
! stat command.
! Repeat this show command until the status is "no actions pending".
```

Further Problem Description: This condition is a timing-related problem that tends to occur with a large dynamic reconfiguration. The workaround avoids the timing-related issue by enforcing atomicity between separate phases of the reconfiguration.

- CSCsz21313

  A Cisco ASR 1000 Series Router reloads with the __be_c3pl_action_account_queueing_stats_free message when removing a subscriber policy with the account feature configured from the port-channel.

  Workaround: Do not configure the account feature within a subscriber policy. The account feature is not supported in Cisco IOS XE Release 2.3.

- CSCsz21732

  A Cisco ASR 1000 Series Router may reload when configured for Simple Network Management Protocol (SNMP) inform notifications.

  Workaround: Disable inform notifications using the **no snmp-server host host-address informs** command.

Resolved Caveats—Cisco IOS XE Release 2.3.1

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.3.1.

- CSCsr16693

  A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

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

  Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

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

- CSCsr29468

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

  Cisco has released free software updates that address this vulnerability.

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

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

- CSCsu21828

  A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

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

  Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

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

- CSCsu38228

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

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

- CSCsv38166

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

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

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

  Cisco has released free software updates that address this vulnerability.

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

  This advisory is posted at the following link:

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

- CSCsv49924

  When multiple Dynamic Host Configuration Protocol (DHCP) Relay agents are present between the clients and the DHCP server, the incorrect binding and route is created on the DHCP Relay Agent.

  There are no known workarounds.

- CSCsv70092

  When executing the **redundancy force-switchover** command in a software redundant configuration on a Cisco ASR 1000 Series Router, the active Route Processor (RP) may experience a kernel driver fault and reload unexpectedly.

  There are no known workarounds; the router will recover after the RP reload.

- CSCsw46873

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

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

  There are no known workarounds.

- CSCsx02650

  On a Cisco ASR 1000 Series Router, malformed IPv4 fragmented packets result in reassembly failure in the virtual fragment reassembly (VFR) feature and are dropped with the following error message:

  ```
  ATTN-3-SYNC_TIMEOUT
  ```

  In addition, the Cisco QuantumFlow Processor (QFP) global drop counters indicate a reassembly failure or timeout.

  There are no known workarounds.

- CSCsx04070

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

  This condition is observed under the following configuration scenario:

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

  where:

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

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

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

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

- CSCsx06021

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

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

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

- CSCsx06507

  If a Packet-over-SONET (POS) SPA experiences a loss of signal failure during a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router, a synchronization mismatch of states may occur between the SPA hardware and the RP. This intermittent condition is observed after the RP switchover if a soft or hard online insertion and removal (OIR) insertion of the SPA is performed. It may affect the functionality of higher level protocols running on the RP.

  There are no known workarounds.

  Further Problem Description: This intermittent condition is caused by a timing issue. It only occurs. when the timing of the SPA reload occurs such that events from the SPA hardware are missed.

- CSCsx10283

  Under rare conditions, the active RP2 on a Cisco ASR 1000 Series Router may reload unexpectedly when online insertion and removal (OIR) is performed on the standby RP.

  There are no known workarounds.

- CSCsx15761

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

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

  Workaround: Prevent resource exhaustion.

- CSCsx17284

  A traffic delay of 10 seconds is observed after a Route Processor (RP) High Availability (HA) switchover on a Packet-over-SONET (POS) interface on a Cisco ASR 1000 Series Router.

  This condition occurs because when the standby RP becomes active, the POS interface is reset.

  There are no known workarounds.

- CSCsx27977

  In an IPSec network on a Cisco ASR 1000 Series Router, Border Gateway Protocol (BGP) routes may not be advertised through Generic Routing Encapsulation (GRE) tunnels.

  This condition has been observed after a Route Processor (RP) switchover or when both IPSec peers are brought up about the same time.

  Workaround: Enable **crypto ipsec frag after-encryption** in the configuration.

- CSCsx33368

  Network Address Translation (NAT) mapping using a route-map with **match interface** does not work on the Cisco ASR 1000 Series Router.

  Workaround: If possible, use **match ip nexthop** in the route-map instead.

- CSCsx39037

  The injected IPv6 or IPv4 data pak from Cisco IOS is not sent out to the Protocol Independent Multicast (PIM) tunnel on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsx51860

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

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

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

- CSCsx55431

  An Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload continuously if an online insertion and removal (OIR) insertion of ESP is performed or the ESP is reloaded while crypto session removals (**clear crypto session** commands) are being processed.

  Workaround: Before performing an ESP OIR or reload, ensure that no outstanding crypto session removals are to be processed by checking the status of the active crypto sessions on the active ESP.

- CSCsx57569

  On a Cisco ASR 1000 Series Router with hierarchical Quality of Service (QoS) applied, an unexpected reload of the Embedded Services Processor (ESP) may occur if the hierarchical policy is repeatedly removed and replaced with another policy.

  This condition occurs if the following scenario is repeated multiple times under highly scaled conditions: first the child policy is removed, then the parent policy is removed, and finally an entirely new/separate hierarchical policy is created. Note that the problem doe s not occur when only the child policy is repeatedly removed and replaced.

  Workaround: Avoid removing the child policy when wholesale QoS configuration changes are required.

- CSCsx60481

  When performing an in-service software upgrade (ISSU) upgrade to or downgrade from Cisco IOS XE Release 2.3.0, the following error messages may appear on the console:

  ```
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_sp:  cpp_sp encountered an error
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp:  cpp_cp encountered an error
  ```

  There is no service impact due to these error messages, and the upgrade/downgrade completes successfully.

  There are no known workarounds.

- CSCsx61701

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

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

- CSCsx62253

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

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

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

- CSCsx63557

  When Layer 2 Tunnel Protocol (L2TP) sessions are created and then torn down by Intelligent Services Gateway (ISG), the Cisco QuantumFlow Processor (QFP) leaks DRAM memory.

  There are no known workarounds.

- CSCsx63585

  On a Cisco ASR 1000 Series Router, the repeated set-up and teardown of large numbers of Intelligent Services Gateway (ISG) sessions over the Layer 2 Tunnel Protocol (L2TP) results in a memory leak on the Embedded Services Processor (ESP). The leak is small, and no service impact is expected under normal operating conditions.

  There are no known workarounds.

- CSCsx63860

  When you perform an in-service software upgrade (ISSU) downgrade to Cisco IOS XE Release 2.3.0 on a Cisco ASR 1000 Series Router containing an operational SPA-4XOC3-POS-V2 SPA, the following messages appear on the active RP console:

  ```
  %IDBINDEX_SYNC-4-RESERVE: Failed to lookup existing ifindex for an  interface on the
  Standby, allocating a new ifindex from the Active (ifindex=58, idbtype=SWIDB)
  ```

  Workaround: Shut down the SPA-4XOC3-POS-V2 SPA before beginning the downgrade process and then bring the SPA back up after the downgrade is complete.

- CSCsx67820

  When a firewall is configured on a Cisco ASR 1000 Series Router and the **no debug platform hardware qfp active feature firewall datapath global all detail** command is issued, a lot of messages may flood the console.

  Workaround: Avoid using the **no debug platform hardware qfp active feature firewall datapath global all detail** command.

- CSCsx68791

  The following traceback is observed on the console of a Cisco ASR 1000 Series Router when a class map is removed and added from a crypto interface:

  ```
  *Feb 12 21:23:45.134: %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread:033
  TS:00000021156554985833 %QOS-3-INVALID_CLASS_QID: Class Queuing error for interface
  TenGigabitEthernet1/3/0.4002, qid 9293 vqid 0 -Traceback= 802437f8 8009fd39 82003612
  8036b9bb 801f6f00 820126ac 80020064 80020055
  *Feb 12 21:23:45.134: %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread:033
  TS:00000021156555178393 %QOS-3-VALID_DEFAULT_QID: Using Default Queue for interface
  TenGigabitEthernet1/3/0.4002, qid 63 vqid 63 -Traceback= 802437f8 8009fdcd 82003612
  8036b9bb 801f6f00 820126ac 80020064 80020055   ent-6ru-2(config-pmap-c)#end
  ```

This message is not observed with regular interfaces.

Workaround: This traceback is transient and harmless. To avoid the traceback when policy map changes are required, perform the following steps: remove the policy map from the interface, make the changes to it, and then reapply the policy map.

- CSCsx71752

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload due to a cpp_cp process failure when using a non-existent ACE ID value in the **show platform hardware qfp active feature ipsec spd** *spdId* **ace** *aceId cgId* command to check IPSec counters.

  Workaround: Use the appropriate ACE ID value returned by the IPSec platform commands.

- CSCsx76396

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when a crypto map is removed from the configuration and the crypto map contains a match for a clear text packet. For example:

```
crypto dynamic-map dyn_map 10
set ip access-group 102 in
set ip access-group 103 out
set transform-set t1
crypto map testmap 10 ipsec-isakmp dynamic dyn_map

interface GigabitEthernet0/0/1
ip address 16.0.0.1 255.255.255
ip access-group 104 in
ip access-group 105 out
no ip unreachables
negotiation auto
crypto map testmap
```

  There are no known workarounds.

- CSCsx76862

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

  There are no known workarounds.

- CSCsx77598

  If the **show platform hardware cpp active feature qos police output interface** *interface-name* command is executed during an in-service software upgrade (ISSU) from Cisco IOS XE Release 2.2 to Cisco IOS XE Release 2.3 on a Cisco ASR 1004 or Cisco ASR 1002 router, the following error message may occur:

```
% Error: QOS transaction processing in progress, try again later
```

  This condition is observed when the router is configured with Quality of Service (QoS) and the command is executed after the Route Processor (RP) is upgraded to Cisco IOS XE Release 2.3 but while the Embedded Services Processor (ESP) is still running the Cisco IOS XE Release 2.2.

  Workaround: Do not issue the **show** command in the middle of the ISSU procedure.

- CSCsx79872

  Under rare conditions, after Network Address Translation (NAT) is completely unconfigured (and not re-configured), a reload of the Cisco ASR 1000 Series Router may occur.

  Workaround: Remove NAT before reloading the router.

- CSCsx80170

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

  There are no known workarounds.

- CSCsx83387

  When performing a downgrade to Cisco IOS XE Release 2.3.0, the standby Cisco IOS process, which is still running Cisco IOS XE Release 2.3.0, fails to start and prevents the downgrade from completing.

  There are no known workarounds.

- CSCsy01886

  On a Cisco ASR 1000 Series Router with an RP2, PPP over Ethernet (PPPoE) subscribers whose sessions terminate at an L2TP Network Server (LNS) fail to authenticate if they have a RADIUS-supplied user profile with an attribute of the type "**lcp:interface-config=**...".
  A Cisco ASR 1000 Series Router with an RP1 is not affected.

  This condition is observed under the following scenario:

  - The "**lcp:interface-config=**... " attribute in a RADIUS user profile is used to configure features on a session. For example, "**lcp:interface-config=zone-member security DoS-max-zone**" is used with a firewall configuration, or "**lcp:interface-config=ip vrf forwarding vrf1**" is used with a VRF forwarding configuration.
  - The zone member for the PPPoE subscriber is downloaded using RADIUS.

  Workaround: Define PPPoE subscriber features in virtual templates.

- CSCsz80074

  Due to a minor change in the build script for Cisco IOS XE Release 2.3.0 and Cisco IOS XE Release 2.3.1, the Cisco IOS XE Release 2.3.0 and Cisco IOS XE Release 2.3.1 images can be 15 to 30 MB larger than intended.

  Workaround: If the image size of Cisco IOS XE Release 2.3.0 or Cisco IOS XE Release 2.3.1 is not causing any issues, no action is necessary, however, these images will no longer be downloadable on Cisco.com. Replacement images (Cisco IOS XE Release 2.3.0t and Cisco IOS XE Release 2.3.1t) with exactly the same content and bug fixes will be available on Cisco.com. Old image MD5 sums will still be available for verification on the download page.

Open Caveats—Cisco IOS XE Release 2.3.0

This section documents possible unexpected behavior by Cisco IOS XE Release 2.3.0.

- CSCsu38228

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

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

- CSCsu52126

  When the **redundancy force-switchover** command is executed from slot 0 to slot 1 on a Cisco ASR 1000 Series Router, the recovery time is several seconds more than when the switchover is done in reverse (from slot 1 to slot 0).

  There is no failure on the switchover, only a delay in the time that the router starts forwarding legacy traffic to or receiving traffic from the new IOSd instance.

  There are no known workarounds.

- CSCsu80584

  During an in-service software upgrade (ISSU) downgrade to the Cisco IOS XE Release 2.3 or Cisco IOS XE Release 2.2 image on a Cisco ASR 1000 Series Router, the following traceback is observed:

  ```
  %FMANRP_OBJID-5-DUPCREATE: Duplicate forwarding object creation obj_handle
  ```

  There are no known workarounds.

- CSCsv49924

  When multiple Dynamic Host Configuration Protocol (DHCP) Relay agents are present between the clients and the DHCP server, the incorrect binding and route is created on the DHCP Relay Agent.

  There are no known workarounds.

- CSCsx06021

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

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

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

- CSCsv69275

  If a Cisco ASR 1000 Series Router cannot successfully perform IPv6 neighbor-discovery, it does not send an ICMP unreachable packet to the originator of the packet.

  There is no known workaround other than configuring static Neighbor Discovery (ND) entries.

- CSCsv70092

  When executing the **redundancy force-switchover** command in a software redundant configuration on a Cisco ASR 1000 Series Router, the active Route Processor (RP) may experience a kernel driver fault and reload unexpectedly.

  There are no known workarounds; the router will recover after the RP reload.

- CSCsv99477

  The following REASSEMBLY_ERR message appears on the IOS console on a Cisco ASR 1000 Series Router:

  ```
  frag info reference counter reaches  zero
  ```

  This condition occurs when Network Address Translation (NAT) is enabled, fragments are received out-of-order, and the Cisco QuantumFlow Processor (QFP) has to drop the packets because it cannot put them in order for NAT. These fragmented packets are most likely dropped.

  There are no known workarounds.

- CSCsw23314

  The Cisco ASR 1000 Series Router reloads when a manual keyed crypto map is removed from an interface after unconfiguring the tunnel source.

  This condition occurs when the user cuts and pastes several "**no**" forms of CLI commands to delete the tunnel source interface, the crypto map from the tunnel, and the tunnel interface itself.

  For example:

```
conf t
int tunnel0
no ip addr x.x.x.x x.x.x.x
no tunnel source e1/0
no tunnel dest y.y.y.y
no crypto map ! must be a manual keyed crypto map
exit
no interface tunnel0
```

  Workaround: Enter the commands one at a time, and wait after removing the tunnel source. This workaround will prevent the race condition from occurring and avoid the reload.

- CSCsw29132

  A group member may not receive retransmit rekeys if any of the following conditions occur:

  - An access control list (ACL) is added to the key server.
  - An ACL is changed on the key server.
  - The retransmit CLI parameter is changed on the key server.

  There are no known workarounds.

- CSCsw39916

  When you remove an IPv4 or IPv6 address from a Session Border Controller (SBC) interface, either directly or indirectly by removing virtual routing and forwarding (VRF) forwarding or VRF definitions, the media addresses or media pools that are configured on the SBC interface remain configured even though these addresses refer to IP addresses that were deleted.

  Possible affected commands include the following:

  no ip address *address mask*

  no ip address

  no ipv6 address *address-specification*

  no ipv6 address

  no vrf forwarding

  no VRF definition *vrf-name*

  Workaround: Remove the media addresses or media pools from the SBC interface before removing or causing the removal of IP addresses on the SBC interface.

  Further Problem Description: Leaving media addresses or media pools configured on an SBC interface after their IP addresses have been removed from the SBC interface may cause routing problems for future calls. If an IP address that was removed is associated with a non-default VRF, then adding back the VRF does not solve the problem. You must unconfigure the SBC interface.

- CSCsw41261

  Under very rare conditions, an RP2 on a Cisco ASR 1000 Series Router may reload during its initial boot because of a missing bootflash device. The following messages are observed on the console:

  ```
  %IOSXEBOOT-4-DEVICE_MISSING: (rp/0): Integrity check for missing device /dev/bootflash
  not performed.  %IOSXEBOOT-1-BOOTFLASH_FAILED_MISSING: (rp/0): Required Bootflash disk
  failed or missing, reloading system
  ```

  These messages are followed by a reload of the RP2. The subsequent reload is successful and the condition appears to clear.

  There are no known workarounds; the system self-recovers.

- CSCsw45701

  Under very rare conditions, an RP2 on a Cisco ASR 1000 Series Router may experience an unexpected reload during intensive file-system operations to the USB-based file systems (bootflash:, usb0:/usb1:).

  Workaround: Limit the USB file-system operations. For example, avoid copying to and from bootflash and to and from external USB sticks.

- CSCsw46873

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

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

  There are no known workarounds.

- CSCsw47239

  A Cisco ASR 1006 Router with an RP2 configured with Route Processor Redundancy (RPR) experiences traffic loss exceeding the expected threshold of 100 seconds on an RP switchover. This issue is not observed with an RP1.

  There are no known workarounds.

  Further Problem Description: In RPR mode, after an RP switchover, the Embedded Services Processors (ESPs) and SIPs are reset. Both the ESPs and the SPAs (which are present in the SIPs) take more than 100 seconds to boot up. During this interval, traffic loss is experienced.

- CSCsw66319

  The following traceback message may be observed on a Cisco ASR 1000 Series Router when you bring up a large number of PPP over Ethernet (PPPoE) sessions with a Quality of Service (QoS) policy applied to them at a high rate of session setup:

  ```
  %QOS-3-INVALID_CLASS_QID
  ```

  There are no known workarounds.

- CSCsw81617

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may unexpectedly restart during a reconfiguration.

  This condition is observed when certain combinations of features are configured concurrently on the same interface, such as the combination of NetFlow and Unicast Reverse Path Forwarding (uRPF).

Workaround: Performing the following steps may help mitigate this issue:

1. Execute a **shut** at the interface.
2. Remove features from the interface.
3. Re-add the desired features to the interface.
4. Execute **no shut** at the interface.

- CSCsw88573

  A process on the standby Route Processor (RP) on a Cisco ASR 1000 Series Router may reload during an in-service software upgrade (ISSU) downgrade from Cisco IOS XE Release 2.3.0 to Cisco IOS XE Release 2.2.2. This condition may also delay new IPSec tunnel establishment. If the process has already been reloaded three times since the IOSd process came online, the IOSd process may also reload.

  This condition occurs when the second RP is to be installed with Cisco IOS XE 2.2.0 software packages after the first RP switchover during the ISSU downgrade process.

  Workaround: If IPSec is deployed, bring down the IPSec tunnels before downgrading from Cisco IOS XE Release 2.3.0.

- CSCsw96044

  The Cisco IOS process on a Cisco ASR 1000 Series Router may reset when virtual routing and forwarding (VRF) forwarding is enabled on a T3 Frame-Relay subinterface after IP address configuration on the interface.

  There are no known workarounds.

- CSCsx01992

  Upgrading the ROMmon image on an RP2 in a Cisco ASR1006 Router may fail when the RP2 is the active RP and in slot 1.

  Workaround: Perform the ROMmon upgrade in slot 0 only, and swap boards to complete the upgrade for both RPs.

- CSCsx02650

  On a Cisco ASR 1000 Series Router, malformed IPv4 fragmented packets result in reassembly failure in the virtual fragment reassembly (VFR) feature and are dropped with the following error message:

  ```
  ATTN-3-SYNC_TIMEOUT
  ```

  In addition, the Cisco QuantumFlow Processor (QFP) global drop counters indicate a reassembly failure or timeout.

  There are no known workarounds.

- CSCsx05516

  The Cisco ASR 1000 Series Router may drop packets with an IP format error if the key server is configured with time based anti-replay and an Embedded Services Processor (ESP) switchover is triggered on the chassis.

  Workaround: Initiate a re-key after every ESP switchover.

- CSCsx06507

  If a Packet-over-SONET (POS) SPA experiences a loss of signal failure during a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router, a synchronization mismatch of states may occur between the SPA hardware and the RP. This intermittent condition is observed after the RP switchover if a soft or hard online insertion and removal (OIR) insertion of the SPA is performed. It may affect the functionality of higher level protocols running on the RP.

  There are no known workarounds.

  Further Problem Description: This intermittent condition is caused by a timing issue. It only occurs. when the timing of the SPA reload occurs such that events from the SPA hardware are missed.

- CSCsx10283

  Under rare conditions, the active RP2 on a Cisco ASR 1000 Series Router may reload unexpectedly when online insertion and removal (OIR) is performed on the standby RP.

  There are no known workarounds.

- 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.

  There are no known workarounds.

- CSCsx15761

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

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

  Workaround: Prevent resource exhaustion.

- CSCsx15768

  The active Route Processor (RP) on a Cisco ASR 1000 Series Router reloads and a core dump is generated when encapsulation is changed from **encapsulation frame-relay** to **no encapsulation frame-relay** on a serial interface.

  This condition occurs under the following scenario:

  – The Cisco ASR 1000 Series Router has **ipv6 multicast-routing** enabled.

  – The router has at least one serial interface configured with **encapsulation frame-relay**.

  – That particular serial interface has both IPv4 and IPv6 addresses configured.

  – The frame-relay encapsulation is removed by executing the **no encapsulation frame-relay** command on the serial interface.

  Workaround: There are two workarounds for this problem:

  1. Remove the IPv6 configuration by executing the **no ipv6 enable** and **no ipv6 address** commands on the serial interface, perform the encapsulation change, and then re-configure the IPv6 configuration.
  2. Shut down the serial interface, remove the frame-relay encapsulation, and then execute **no shutdown** on the interface.

- CSCsx17284

  A traffic delay of 10 seconds is observed after a Route Processor (RP) High Availability (HA) switchover on a Packet-over-SONET (POS) interface on a Cisco ASR 1000 Series Router.

  This condition occurs because when the standby RP becomes active, the POS interface is reset.

  There are no known workarounds.

- CSCsx18983

  When a Quality of Service (QoS) parent policy with 256 class maps is applied and removed from an interface on a Cisco ASR 1000 Series Router, the CPPOSLIB-3-ERROR_NOTIFY error message is generated and traceback is observed on the console. There is no service impact due to this error message.

  There are no known workarounds.

- CSCsx26324

  If an RP2 ROMmon upgrade on the Cisco ASR 1000 Series Router fails to boot the newly installed ROMmon, the router continues to attempt to boot using the failed ROMmon.

  This condition occurs only if the newly installed ROMmon cannot successfully initialize itself and reach the ROMmon prompt.

  Workaround: When the router returns to the ROMmon prompt after exhausting the maximum number of boot attempts, the upgrade pending setting can be cleared manually from the ROMmon CLI by executing the **priv**, **clrdip**, and **reset** commands in sequence. After executing these commands, the router should be able to boot using the previously installed ROMmon.

- CSCsx27977

  In an IPSec network on a Cisco ASR 1000 Series Router, Border Gateway Protocol (BGP) routes may not be advertised through Generic Routing Encapsulation (GRE) tunnels.

  This condition has been observed after a Route Processor (RP) switchover or when both IPSec peers are brought up about the same time.

  Workaround: Enable **crypto ipsec frag after-encryption** in the configuration.

- CSCsx30747

  During an in-service software upgrade (ISSU) from Cisco IOS XE Release 2.2.2 to Cisco IOS XE Release 2.3.0 on a Cisco ASR 1000 Series Router, the following error message may be generated:

  ```
  %FMANRP_OBJID-5-DUPCREATE
  ```

  This condition may occur because of a race condition on the serial subinterfaces between Frame-Relay encapsulation and configuring/unconfiguring IPv4 andIPv6 addresses.

  There are no known workarounds.

- CSCsx33368

  Network Address Translation (NAT) mapping using a route-map with **match interface** does not work on the Cisco ASR 1000 Series Router.

  Workaround: If possible, use **match ip nexthop** in the route-map instead.

- CSCsx35419

  On a Cisco ASR 1000 Series Router, the Enhanced Interior Gateway Routing Protocol (EIGRP) may flap on Dynamic Multipoint VPN (DMVPN) tunnels with tunnel protection configured.

  This condition may occur when the EIGRP control traffic has a packet size that is greater than the tunnel interface maximum transmission unit (MTU) and tunnel protection is configured.

  Workaround: Do not use tunnel protection when the EIGRP packet size can be greater than the tunnel interface MTU.

- CSCsx39037

  The injected IPv6 or IPv4 data pak from Cisco IOS is not sent out to the Protocol Independent Multicast (PIM) tunnel on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsx46099

  Under rare conditions, when there is a Cisco QuantumFlow Processor (QFP) fault and subsequent core dump on a Cisco ASR 1000 Series Router, the affected Embedded Services Processor (ESP) may experience a secondary kernel fault during the shutdown/reload of the ESP. This condition increases the time for the ESP to reload up to 10 minutes.

  There are no known workarounds. The affected ESP will restart normally after the kernel fault generates a core dump.

- CSCsx47529

  Under rare conditions, a defective hard disk drive may cause the RP2 on a Cisco ASR 1000 Series Router to hang indefinitely during startup.

  Workaround: Remove the defective hard disk from the RP2 and power cycle the RP2. The RP2 should start successfully with reduced functionality (no persistent logging or core dump collection). Request a return materials authorization (RMA) for the defective hard disk drive.

- CSCsx48566

  When the same child policy is used by two hierarchical parent policies that have different output in a broadband Quality of Service (QoS) configuration on a Cisco ASR 1000 Series Router, and the Change of Authorization (CoA) tool is used to change the session output qos hierarchical policy, the CPPOSLIB-3-ERROR_NOTIFY message appears on the console.

  Workaround: Define individual child polices for each of the parent policies.

- CSCsx51265

  When a Route Processor (RP) on a Cisco ASR 1000 Series Router is reloaded with a Quality of Service (QoS) policy that has 256 class maps contained in the policy and this policy is applied to a crypto interface, traceback is observed at cpp_bqs_mgr_lib.

  There are no known workarounds.

- CSCsx51860

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

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

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

- CSCsx55431

  An Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload continuously if an online insertion and removal (OIR) insertion of ESP is performed or the ESP is reloaded while crypto session removals (**clear crypto session** commands) are being processed.

  Workaround: Before performing an ESP OIR or reload, ensure that no outstanding crypto session removals are to be processed by checking the status of the active crypto sessions on the active ESP.

- CSCsx57569

  On a Cisco ASR 1000 Series Router with hierarchical Quality of Service (QoS) applied, an unexpected reload of the Embedded Services Processor (ESP) may occur if the hierarchical policy is repeatedly removed and replaced with another policy.

  This condition occurs if the following scenario is repeated multiple times under highly scaled conditions: first the child policy is removed, then the parent policy is removed, and finally an entirely new/separate hierarchical policy is created. Note that the problem doe s not occur when only the child policy is repeatedly removed and replaced.

  Workaround: Avoid removing the child policy when wholesale QoS configuration changes are required.

- CSCsx57787

  In a large IPSec configuration (such as 1K Generic Routing Encapsulation (GRE) tunnels) on a Cisco ASR 1000 Series Router, the standby Embedded Services Processor (ESP) may reload during a Route Processor (RP) switchover.

  This condition may occur when **tunnel protection ipsec profile** is configured on the GRE tunnel interfaces in scaled configurations of 1K GRE tunnels. The standby ESP may reload after the RP switchover if the switchover is initiated by the active RP on slot 1.

  There are no known workarounds.

- CSCsx58136

  The following message may appear during a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router:

  ```
  %PMAN-3-PROCHOLDDOWN: F0: pman.sh: The process fman_fp_image has been helddown
  ```

  This condition can occur when a router with dual RPs is configured with Stateful Switchover (SSO) and a Quality of Service (QoS) policy.

  There are no known workarounds.

- CSCsx60175

  When IPv6 multicast packets are sent through IPv6-over-IPv4 tunnels on a Cisco ASR 1000 Series Router, the IPv6 packets are sent as register packets, not as native packets.

  There are no known workarounds.

- CSCsx60481

  When performing an in-service software upgrade (ISSU) upgrade to or downgrade from Cisco IOS XE Release 2.3.0, the following error messages may appear on the console:

  ```
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_sp:  cpp_sp encountered an error
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp:  cpp_cp encountered an error
  ```

  There is no service impact due to these error messages, and the upgrade/downgrade completes successfully.

  There are no known workarounds.

- CSCsx61692

  The Cisco ASR 1000 Series Router does not respond with a valid Router Advertisement and IPv6 prefix when the packet receives an ALL-ROUTER-MULTICAST address packet.

  There are no known workarounds.

- CSCsx61701

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

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

- CSCsx62253

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

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

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

- CSCsx62653

  When in-service software upgrade (ISSU) is performed, ISSU-related objects in the CISCO-RF-MIB return null strings.

  Workaround: Use the **show issu state detail** command instead.

- CSCsx63557

  When Layer 2 Tunnel Protocol (L2TP) sessions are created and then torn down by Intelligent Services Gateway (ISG), the Cisco QuantumFlow Processor (QFP) leaks DRAM memory.

  There are no known workarounds.

- CSCsx63585

  On a Cisco ASR 1000 Series Router, the repeated set-up and teardown of large numbers of Intelligent Services Gateway (ISG) sessions over the Layer 2 Tunnel Protocol (L2TP) results in a memory leak on the Embedded Services Processor (ESP). The leak is small, and no service impact is expected under normal operating conditions.

  There are no known workarounds.

- CSCsx63860

  When you perform an in-service software upgrade (ISSU) downgrade to Cisco IOS XE Release 2.3.0 on a Cisco ASR 1000 Series Router containing an operational SPA-4XOC3-POS-V2 SPA, the following messages appear on the active RP console:

  ```
  %IDBINDEX_SYNC-4-RESERVE: Failed to lookup existing ifindex for an  interface on the
  Standby, allocating a new ifindex from the Active (ifindex=58, idbtype=SWIDB)
  ```

  Workaround: Shut down the SPA-4XOC3-POS-V2 SPA before beginning the downgrade process and then bring the SPA back up after the downgrade is complete.

- CSCsx64518

  Using jumbo frames (greater than 18000 bytes) on the management Ethernet port of the RP2 on a Cisco ASR 1000 Series Router may cause the resulting frames to be dropped and the following buffer error to be generated:

  ```
  %SYS-2-INPUT_GETBUF: Bad getbuffer, bytes= 18030, for interface= GigabitEthernet0
  ```

  Workaround: Reduce the size of frames on the management Ethernet network to less than 18K in size.

- CSCsx67122

  The console baud rate of an RP2 on a Cisco ASR 1000 Series Router does not function properly when set to speeds other than default value of 9600 baud.

  This condition is observed when the console baud rate is changed either in the ROMmon or in the Cisco IOS configuration.

  Workaround: Do not configure baud rates other than default value of 9600 baud on the console.

- CSCsx67820

  When a firewall is configured on a Cisco ASR 1000 Series Router and the **no debug platform hardware qfp active feature firewall datapath global all detail** command is issued, a lot of messages may flood the console.

  Workaround: Avoid using the **no debug platform hardware qfp active feature firewall datapath global all detail** command.

- CSCsx68133

  The output of the **show policy-map type inspect zone-pair** *zone-pair-name* **session** command on a Cisco ASR 1000 Series Router displays some packet counts without protocol names.

  This condition is observed when a firewall is configured, a class map is being modified while in use, the policy is attached to a zone-pair, and the class map is experiencing high traffic.

  Workaround: Execute the **clear zone-pair** *zone-pair-name* **counter** command to clear the irregular counters.

- CSCsx68348

  When the **loadversion** command is issued for an RP package (on slot 0), the changed software fails to start.

  This condition is intermittent.

  There are no known workarounds.

- CSCsx68791

  The following traceback is observed on the console of a Cisco ASR 1000 Series Router when a class map is removed and added from a crypto interface:

  ```
  *Feb 12 21:23:45.134: %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread:033
  TS:00000021156554985833 %QOS-3-INVALID_CLASS_QID: Class Queuing error for interface
  TenGigabitEthernet1/3/0.4002, qid 9293 vqid 0 -Traceback= 802437f8 8009fd39 82003612
  8036b9bb 801f6f00 820126ac 80020064 80020055
  *Feb 12 21:23:45.134: %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread:033
  TS:00000021156555178393 %QOS-3-VALID_DEFAULT_QID: Using Default Queue for interface
  TenGigabitEthernet1/3/0.4002, qid 63 vqid 63 -Traceback= 802437f8 8009fdcd 82003612
  8036b9bb 801f6f00 820126ac 80020064 80020055   ent-6ru-2(config-pmap-c)#end
  ```

This message is not observed with regular interfaces.

Workaround: This traceback is transient and harmless. To avoid the traceback when policy map changes are required, perform the following steps: remove the policy map from the interface, make the changes to it, and then reapply the policy map.

- CSCsx68821

  On a Cisco Systems ASR 1000 Series Router with hierarchical Quality of Service (QoS) applied, an unexpected reload of the Embedded Services Processor (ESP) may occur if the hierarchical policy is removed and re-attached.

  This condition occurs when hierarchical QoS is applied on a subinterface that has multiple Generic Routing Encapsulation (GRE) tunnels.

  Workaround: Avoid removing and re-attaching a hierarchical policy map on a subinterface with multiple GRE tunnels.

- CSCsx71472

  Interface names may be improperly filtered on a Cisco ASR 1000 Series Router running NetFlow. This condition can cause interfaces to appear to have flows that really do not exist and are actually present on a different interface. For example, flows may appear to be present on interfaces that do not have NetFlow configured.

  This condition can be observed by executing the **show ip cache** *interface* **flow** command. This issue does not impact exported flows; it only impacts flows shown on the router console.

  There are no known workarounds. This bug is cosmetic.

- CSCsx71660

  When the **test platform hardware slot r1 oir power-cycle** command is executed on a Cisco ASR 1000 Series Router, the Route Processor (RP) goes into the disabled state.

  There are no known workarounds.

- CSCsx71752

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload due to a cpp_cp process failure when using a non-existent ACE ID value in the **show platform hardware qfp active feature ipsec spd** *spdId* **ace** *aceId cgId* command to check IPSec counters.

  Workaround: Use the appropriate ACE ID value returned by the IPSec platform commands.

- CSCsx73902

  When match protocols are removed from an already applied policy-map (class_zone_1) on a Cisco ASR 1000 Series Router, sessions are not cleared even after clearing the sessions multiple times. The expectation is that after the class-map matching protocols are removed, the traffic should pass through the class-default. Even after clearing the sessions, some sessions are still established in the class-map (class_zone_1).

  This condition is observed when Zone-Based Firewall has High Availability (HA) enabled (that is, the standby Embedded Services Processor (ESP) is enabled). When HA is disabled (that is, the standby ESP is in the disabled state), the condition is not observed.

  Workaround: Reload the ESPs.

- CSCsx76396

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when a crypto map is removed from the configuration and the crypto map contains a match for a clear text packet. For example:

```
crypto dynamic-map dyn_map 10
set ip access-group 102 in
set ip access-group 103 out
set transform-set t1
crypto map testmap 10 ipsec-isakmp dynamic dyn_map

interface GigabitEthernet0/0/1
ip address 16.0.0.1 255.255.255
ip access-group 104 in
ip access-group 105 out
no ip unreachables
negotiation auto
crypto map testmap
```

  There are no known workarounds.

- CSCsx76862

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

  There are no known workarounds.

- CSCsx77598

  If the **show platform hardware cpp active feature qos police output interface** *interface-name* command is executed during an in-service software upgrade (ISSU) from Cisco IOS XE Release 2.2 to Cisco IOS XE Release 2.3 on a Cisco ASR 1004 or Cisco ASR 1002 router, the following error message may occur:

```
% Error: QOS transaction processing in progress, try again later
```

  This condition is observed when the router is configured with Quality of Service (QoS) and the command is executed after the Route Processor (RP) is upgraded to Cisco IOS XE Release 2.3 but while the Embedded Services Processor (ESP) is still running the Cisco IOS XE Release 2.2.

  Workaround: Do not issue the **show** command in the middle of the ISSU procedure.

- CSCsx78315

  If tunnel mode is changed from **gre multipoint** to **gre ip** while traffic is passing though the tunnel interface on a Cisco ASR 1000 Series Router, the IOSd process may reset.

  There are no known workarounds.

- CSCsx79872

  Under rare conditions, after Network Address Translation (NAT) is completely unconfigured (and not re-configured), a reload of the Cisco ASR 1000 Series Router may occur.

  Workaround: Remove NAT before reloading the router.

- CSCsx80170

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

  There are no known workarounds.

- CSCsx83387

  When performing a downgrade to Cisco IOS XE Release 2.3.0, the standby Cisco IOS process, which is still running Cisco IOS XE Release 2.3.0, fails to start and prevents the downgrade from completing.

  There are no known workarounds.

- CSCsy01886

  On a Cisco ASR 1000 Series Router with an RP2, PPP over Ethernet (PPPoE) subscribers whose sessions terminate at an L2TP Network Server (LNS) fail to authenticate if they have a RADIUS-supplied user profile with an attribute of the type "**lcp:interface-config=**...".
  A Cisco ASR 1000 Series Router with an RP1 is not affected.

  This condition is observed under the following scenario:

  – The "**lcp:interface-config=**... " attribute in a RADIUS user profile is used to configure features on a session. For example, "**lcp:interface-config=zone-member security DoS-max-zone**" is used with a firewall configuration, or "**lcp:interface-config=ip vrf forwarding vrf1**" is used with a VRF forwarding configuration.

  – The zone member for the PPPoE subscriber is downloaded using RADIUS.

  Workaround: Define PPPoE subscriber features in virtual templates.

Release 2.2 Caveats

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

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

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

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

This section consists of the following subsections:

Open Caveats—Cisco IOS XE Release 2.2.3

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

- CSCek77178

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

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

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

- CSCsj78195

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

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

- CSCsm98756

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

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

- CSCso09886

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

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

  There are no known workarounds.

- CSCso80547

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

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

  There are no known workarounds.

- CSCsq70140

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

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

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

  There are no known workarounds.

- CSCsq73935

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

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

- CSCsq76871

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

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

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

  For example:

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

- CSCsq77838

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

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

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

- CSCsq91659

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

  There are no known workarounds.

- CSCsr22866

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

  There are no known workarounds.

- CSCsr50040

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

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

- CSCsr68177

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

  Workaround: Remove VRF configurations from the interface.

- CSCsr81066

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

  There are no known workarounds.

- CSCsr87974

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

  There are no known workarounds.

- CSCsr90264

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

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

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

- CSCsr95180

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

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

  There are no known workarounds.

- CSCsu44557

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

  There are no known workarounds.

- CSCsu45138

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

  There are no known workarounds.

- CSCsu59865

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

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

- CSCsv38148

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

  There are no known workarounds.

- CSCsv47212

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

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

  There are no known workarounds.

- CSCsv61458

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

  There are no known workarounds.

- CSCsv66694

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

  There are no known workarounds.

- CSCsv79583

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

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

  There are no known workarounds.

- CSCsw15883

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

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

  There are no known workarounds.

- CSCsw33109

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

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

- CSCsw38686/CSCsw71222

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

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

- CSCsw46873

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

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

  There are no known workarounds.

- CSCsw69695

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

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

- CSCsw72162

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

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

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

- CSCsw75587

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

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

- CSCsx04070

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

  This condition is observed under the following configuration scenario:

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

  where:

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

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

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

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

- CSCsx13442

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

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

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

- CSCsx15761

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

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

  Workaround: Prevent resource exhaustion.

- CSCsx18270

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

  There are no known workarounds.

- CSCsx23880

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

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

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

- CSCsx25994

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

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

  There are no known workarounds.

- CSCsx26096

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

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

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

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

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

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

  you would configure:

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

- CSCsx41851

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

  This condition occurs under the following configuration scenario:

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

  There are no known workarounds.

- CSCsx45412

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

  There are no known workarounds.

- CSCsx46513

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

  Workaround: Reduce the scale of your configuration.

- CSCsx46721

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

  There are no known workarounds.

- CSCsx47069

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

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

  There are no known workarounds.

- CSCsx48349

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

  This condition is observed under the following scenario:

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

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

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

- CSCsx50568

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

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

- CSCsx51695

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

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

  There are no known workarounds.

- CSCsx51860

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

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

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

- CSCsx56379

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

  There are no known workarounds.

- CSCsx60439

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

  ```
  QED_QED_LDC_LEAF_INT_INT_LDC_LCOMPUTE_ENG_MAX_SCH_ERR
  PQS_PQS_LOGIC1_INTR_LEAF_INT_INT_CACHE_STATUS_TIME_OUT_ERR_D1
  ```

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

- CSCsx61701

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

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

- CSCsx62253

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

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

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

- CSCsx65975

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

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

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

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

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

- CSCsx66227

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

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

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

- CSCsx66736

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

  There are no known workarounds.

- CSCsx68883

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

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

- CSCsx74979

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

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

- CSCsx76017

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

  Workaround: Reload the ESP manually.

- CSCsx76169

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

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

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

- CSCsx76862

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

  There are no known workarounds.

- CSCsx80170

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

  There are no known workarounds.

- CSCsx99319

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

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

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

  with the following configuration instead:

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

Resolved Caveats—Cisco IOS XE Release 2.2.3

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

- CSCec51750

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

  There are no known workarounds.

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

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

- CSCsc94969

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

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

  There are no known workarounds.

- CSCse29570

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

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

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

- CSCsf25722

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

  Workaround: Do not use SCP to transfer files.

- CSCsh58099

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

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

  There are no known workarounds.

- CSCsj12254

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

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

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

  Workaround: Clear the session.

- CSCsj45031

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

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

- CSCsk25046

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

  Workaround: Remove the policy on the control plane.

- CSCsk49835

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

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

  There are no known workarounds.

- CSCsl24449

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

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

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

  There are no known workarounds.

- CSCsl29214

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

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

  There are no known workarounds.

- CSCsl63494

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

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

  Workaround: Consider removing the max session limit.

- CSCsm50317

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

  Workaround: Remove the policy and re-apply it.

- CSCsm55629

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

  There are no known workarounds.

- CSCsm69981

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

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

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

- CSCsm85137

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

  There are no known workarounds.

- CSCso04657

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

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

- CSCso45720

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

  There are no known workarounds.

- CSCso50347

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

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

- CSCso50671

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

  There are no known workarounds.

- CSCso82707

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

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

  There are no known workarounds.

- CSCso90970

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

  There are no known workarounds.

- CSCsq29198

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

  There are no known workarounds.

- CSCsq31958

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

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

- CSCsq59784

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

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

  There are no known workarounds.

- CSCsq75350

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

  There are no known workarounds.

- CSCsq88370

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

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

- CSCsr06282

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

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

- CSCsr29468

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

  Cisco has released free software updates that address this vulnerability.

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

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

- CSCsr39272

  The following SPA error has been reported:

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

  There are no known workarounds.

- CSCsr51820

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

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

  There are no known workarounds with tunnel-protection enabled.

- CSCsr56358

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

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

  There are no known workarounds.

- CSCsr64012

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

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

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

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

- CSCsr68545

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

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

  There are no known workarounds.

- CSCsr72527

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

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

  There are no known workarounds.

- CSCsr76893

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

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

  Workaround: Move the RP to the hub router.

- CSCsr94507

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

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

  There are no known workarounds.

- CSCsr96049

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

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

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

- CSCsu26526

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

  There are no known workarounds.

- CSCsu38228

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

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

- CSCsu40536

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

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

- CSCsu48898

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

  There are no known workarounds.

- CSCsu50406

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

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

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

- CSCsu50921

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

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

- CSCsu55070

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

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

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

- CSCsu72815

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

  Workaround: Disable ip virtual reassembly.

- CSCsu83925

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

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

- CSCsu84714

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

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

- CSCsu89555

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

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

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

- CSCsu93126

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

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

- CSCsu95355

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

  Workaround: Use a static IP address for the interface.

- CSCsu96325

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

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

- CSCsv04674

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

  There are no known workarounds.

- CSCsv06503

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

  There are no known workarounds.

- CSCsv09347

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

  There are no known workarounds.

- CSCsv09833

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

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

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

- CSCsv14100

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

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

  There are no known workarounds.

- CSCsv14986

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

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

  There are no known workarounds.

- CSCsv15063

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

  There are no known workarounds.

- CSCsv15931

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

  There are no known workarounds.

- CSCsv17521

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

  There are no known workarounds.

- CSCsv18533

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

  ```
  error INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0
  ```

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

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

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

  There are no known workarounds.

- CSCsv22769

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

  There are no known workarounds.

- CSCsv30556

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

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

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

- CSCsv32313

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

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

  Workaround: Move the RP to the hub router.

- CSCsv38166

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

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

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

  Cisco has released free software updates that address this vulnerability.

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

  This advisory is posted at the following link:

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

- CSCsv39880

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

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

- CSCsv47580

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

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

- CSCsv52140

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

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

- CSCsv53908

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

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

  There are no known workarounds.

- CSCsv58823

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

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

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

- CSCsv60491

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

  There are no known workarounds.

- CSCsv61175

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

  There are no known workarounds.

- CSCsv64188

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

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

- CSCsv64997

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

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

  Workaround: Reload the field replaceable unit (FRU).

- CSCsv73388

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

  There are no known workarounds.

- CSCsv73509

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

  This condition is observed under a VTY configuration.

  There are no known workarounds.

- CSCsv80892

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

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

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

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

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

  Workaround: Connect the aux port to a peripheral device.

- CSCsv85639

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

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

- CSCsv86561

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

  There are no known workarounds.

- CSCsv86784

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

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

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

- CSCsv87997

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

  There are no known workarounds.

- CSCsv92307

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

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

- CSCsv93452

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

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

- CSCsv94909

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

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

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

- CSCsv95826

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

  There are no known workarounds.

- CSCsv98491

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

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

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

- CSCsv99429

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

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

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

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

- CSCsw14643

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

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

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

- CSCsw18583

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

  There are no known workarounds.

- CSCsw21000

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

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

  There are no known workarounds.

- CSCsw21831

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

  This condition is indicated by mismatched internal ref counter values.

  There are no known workarounds.

- CSCsw22120

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

  There are no known workarounds.

- CSCsw25478

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

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

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

- CSCsw25750

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

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

  Workaround: Make ESP0 the active ESP in both peers.

- CSCsw28547

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

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

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

- CSCsw33573

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

  There are no known workarounds.

- CSCsw33702

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

  There are no known workarounds

- CSCsw33723

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

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

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

Workaround: Possible workarounds include the following:

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

- CSCsw34175

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

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

- CSCsw36300

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

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

- CSCsw36322

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

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

  Workaround: Avoid issuing the commands.

- CSCsw38227

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

  There are no known workarounds.

- CSCsw40048

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

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

- CSCsw40607

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

  There are no known workarounds.

- CSCsw40203

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

  There are no known workarounds.

- CSCsw40991

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

  There are no known workarounds.

- CSCsw41411

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

  There are no known workarounds.

- CSCsw48224

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

  There are no known workarounds.

- CSCsw74470

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

  There are no known workarounds.

- CSCsw75040

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

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

- CSCsw75233

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

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

  There are no known workarounds.

- CSCsw75411

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

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

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

- CSCsw76109

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

  There are no known workarounds.

- CSCsw78939

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

  There are no known workarounds.

- CSCsw96303

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

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

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

- CSCsw98381

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

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

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

- CSCsw99067

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

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

  For example:

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

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

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

- CSCsx03219

  A Cisco router allows less sessions then configured.

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

  There are no known workarounds.

- CSCsx06021

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

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

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

- CSCsx07225

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

  There are no known workarounds.

- CSCsx14984

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

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

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

- CSCsx17676

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

  There are no known workarounds.

- CSCsx35393

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

  There are no known workarounds.

- CSCsx52309

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

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

  There are no known workarounds.

- CSCsx57899

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

  There are no known workarounds.

- CSCsx63929

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

  ```
  GTRMP_GTR_OTHER_LEAF_INT_INT_SDMA_VITAL_SW_ERR
  ```

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

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

- CSCsx64746

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

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

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

  Workaround: There are two possible workarounds for this problem:

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

Open Caveats—Cisco IOS XE Release 2.2.2

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

- CSCsj78195

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

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

- CSCsl24449

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

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

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

  There are no known workarounds.

- CSCsm98756

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

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

- CSCso18963

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

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

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

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

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

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

- CSCso41804

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

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

- CSCsq37627

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

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

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

- CSCsr00490

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

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

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

- CSCsr01097

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

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

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

- CSCsr10774

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

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

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

- CSCsr18279

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

  There are no known workarounds.

- CSCsr72674

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

  There are no known workarounds.

- CSCsr72527

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

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

  There are no known workarounds.

- CSCsr85028

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

  There are no known workarounds.

- CSCsr90357

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

  There are no known workarounds.

- CSCsr96049

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

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

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

- CSCsr96219

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

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

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

  There are no known workarounds.

- CSCsr97633

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

  This condition causes traffic drop.

  There are no known workarounds.

- CSCsu06783

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

  This condition is observed under the following scenario:

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

  There are no known workarounds.

- CSCsu35640

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

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

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

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

- CSCsu38228

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

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

- CSCsu44557

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

  There are no known workarounds.

- CSCsu47716

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

  There are no known workarounds.

- CSCsu48364

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

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

  There are no known workarounds.

- CSCsu50406

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

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

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

- CSCsu50921

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

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

- CSCsu70289

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

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

- CSCsu72541

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

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

  There are no known workarounds.

- CSCsu75596

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

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

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

- CSCsu80130

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

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

  This condition occurs under the following configuration scenario:

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

  There are no known workarounds.

- CSCsu80736

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

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

- CSCsu88004

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

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

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

- CSCsu89555

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

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

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

- CSCsu93848

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

  There are no known workarounds.

- CSCsv01783

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

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

  There are no known workarounds.

- CSCsv06503

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

  There are no known workarounds.

- CSCsv06863

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

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

- CSCsv09833

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

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

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

- CSCsv09874

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

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

  There are no known workarounds.

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

- CSCsv11231

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

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

- CSCsv14986

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

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

  There are no known workarounds.

- CSCsv17521

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

  There are no known workarounds.

- CSCsv18533

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

  ```
  error INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0
  ```

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

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

  There are no known workarounds.

- CSCsv21712

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

  There are no known workarounds.

- CSCsv21861

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

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

  There are no known workarounds.

- CSCsv22428

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

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

  There are no known workarounds.

- CSCsv22769

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

  There are no known workarounds.

Resolved Caveats—Cisco IOS XE Release 2.2.2

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

- CSCsl08954

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

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

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

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

- CSCsr22845

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

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

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

- CSCsr36498

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

  There are no known workarounds.

- CSCsr41741

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

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

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

- CSCsr51820

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

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

  There are no known workarounds with tunnel-protection enabled.

- CSCsr51882

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

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

- CSCsr52410

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

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

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

- CSCsr58520

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

  This condition occur under the following scenario:

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

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

- CSCsr60513

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

  There are no known workarounds.

- CSCsr66075

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

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

  In addition to this message, packets are dropped.

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

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

- CSCsr67820

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

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

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

  There are no known workarounds.

- CSCsr75239

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

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

  There are no known workarounds.

- CSCsr87300

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

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

  There are no known workarounds.

- CSCsr91559

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

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

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

- CSCsr96652

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

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

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

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

  There are no known workarounds.

- CSCsr99959

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

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

  There are no known workarounds.

- CSCsr99992

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

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

  There are no known workarounds.

- CSCsq13127

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

  There are no known workarounds.

- CSCsu05743

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

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

  There are no known workarounds; this condition is benign.

- CSCsu05477

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

  There are no workarounds.

- CSCsu10336

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

  There are no known workarounds.

- CSCsu13500

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

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

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

- CSCsu25738

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

  There are no known workarounds.

- CSCsu27642

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

  This condition occurs under the following scenario:

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

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

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

- CSCsu27824

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

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

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

- CSCsu27878

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

  There are no known workarounds.

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

- CSCsu33792

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

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

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

- CSCsu35558

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

  There are no known workarounds.

- CSCsu35829

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

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

  There are no known workarounds.

- CSCsu36903

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

  There are no known workarounds.

- CSCsu36908

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

  There are no known workarounds.

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

- CSCsu38990

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

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

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

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

- CSCsu41375

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

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

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

  There are no known workarounds.

- CSCsu41444

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

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

  Workaround: Reduce the number of VRFs and prefixes.

- CSCsu43408

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

  There are no known workarounds.

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

- CSCsu44885

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

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

- CSCsu47120

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

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

- CSCsu48111

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

  This condition occurs under the following scenario:

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

  There are no known workarounds.

- CSCsu49327

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

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

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

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

- CSCsu59082

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

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

- CSCsu61385

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

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

- CSCsu61454

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

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

  ip multicast redundancy nsf holdtime *delay*

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

- CSCsu64094

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

  There are no known workarounds.

- CSCsu67138

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

  There are no known workarounds.

- CSCsu67864

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

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

- CSCsu73720

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

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

  There are no known workarounds.

- CSCsu83876

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

  There are no known workarounds.

- CSCsu83925

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

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

- CSCsu92950

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

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

  There are no known workarounds.

- CSCsu96316

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

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

  There are no known workarounds.

- CSCsu99065

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

  There are no known workarounds.

- CSCsv58823

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

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

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

Open Caveats—Cisco IOS XE Release 2.2.1

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

- CSCsl08954

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

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

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

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

- CSCsm16288

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

  There are no known workarounds.

- CSCso09886

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

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

  There are no known workarounds.

- CSCso34979

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

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

  There are no known workarounds.

- CSCso80547

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

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

  There are no known workarounds.

- CSCsq10217

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

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

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

  There are no known workarounds.

- CSCsq11257

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

  There are no known workarounds.

- CSCsq67414

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

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

  There are no known workarounds.

- CSCsq69183

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

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

There are no known workarounds.

- CSCsq70140

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

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

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

  There are no known workarounds.

- CSCsq73935

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

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

- CSCsq76871

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

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

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

  For example:

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

- CSCsq77104

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

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

- CSCsq78536

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

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

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

- CSCsq83554

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

  There are no known workarounds.

- CSCsq91659

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

  There are no known workarounds.

- CSCsq93212

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

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

- CSCsr10631

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

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

  There are no known workarounds.

- CSCsr10774

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

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

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

- CSCsr18279

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

  There are no known workarounds.

- CSCsr22845

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

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

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

- CSCsr24160

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

  There are no known workarounds.

- CSCsr27155

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

  ```
  ASR1000_RP_DPIDB-3-IDXLOOKUPFAILED
  ```

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

  There are no known workarounds.

- CSCsr41741

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

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

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

- CSCsr43311

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

  There are no known workarounds.

- CSCsr45682

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

  This condition may impact desirable QoS behaviors.

  There are no known workarounds.

- CSCsr46529

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

  There are no known workarounds.

- CSCsr50040

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

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

- CSCsr51820

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

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

  There are no known workarounds with tunnel-protection enabled.

- CSCsr53729

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

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

  There are no known workarounds.

- CSCsr55626

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

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

  There are no known workarounds.

- CSCsr56358

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

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

  There are no known workarounds.

- CSCsr59527

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

  There are no known workarounds.

- CSCsr68177

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

  Workaround: Remove VRF configurations from the interface.

- CSCsr72171

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

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

  There are no known workarounds.

- CSCsr75239

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

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

  There are no known workarounds.

- CSCsr76562

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

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

  There are no known workarounds.

- CSCsr81066

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

  There are no known workarounds.

- CSCsr85028

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

  There are no known workarounds.

- CSCsr85690

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

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

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

  There are no known workarounds.

- CSCsr85737

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

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

  There are no known workarounds.

- CSCsr87974

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

  There are no known workarounds.

- CSCsr88298

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

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

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

- CSCsr89529

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

  Workaround: Reload the SPA.

- CSCsr90264

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

  Zoning is currently not configured for interface Virtual-Access

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

- CSCsr91559

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

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

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

- CSCsr92450

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

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

  There are no known workarounds.

- CSCsr92883

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

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

  There are no known workarounds.

- CSCsr92999

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

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

- CSCsr94074

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

  This condition may cause the interface to drop traffic.

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

- CSCsr95924

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

  ```
  Aug 14 11:11:33.037: %SYS-3-CPUHOG: Task is running for (2023)msecs, more than
  (2000)msecs (12/12),process = IPC LC Message Handler.
  ```

  This condition occurs with a Multiprotocol Label Switching (MPLS) Layer 3 VPN (L3VPN) configuration that consists of large numbers of VPNs and Border Gateway Protocol (BGP) peers.

  The traceback has no functional impact.

  Workaround: Disable the SNMP trap for the CEF peer-fib-state-change by removing the following line from the configuration: **snmp-server enable traps cef peer-fib-state-change**.

- CSCsr95653

  A Cisco ASR 1000 Series Router may experience more than 100ms turnaround times (TATs) or message response latencies for H.248 Session Border Controller (SBC) requests.

  There are no known workarounds.

- CSCsr96219

  A Cisco ASR 1000 Series Router configured with ip virtual-reassembly, ip nat outside, and frame relay fragmentation on an interface/subinterface generates the following error message:

  ```
  %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread:044 TS:00000004308774891044
  %ATTN-3-SYNC_TIMEOUT: msecs since last timeout 4304017, missing packets 1
  ```

  The error message does not necessarily mean a packet is physically missing; it can indicate an internal bug of packet tracking in the system.

  There are no known workarounds.

- CSCsr96652

  When a Cisco 8-Port Gigabit Ethernet SPA (SPA-8X1GE-V2) is stopped or removed on a Cisco ASR 1000 Series Router, and the standby RP is rebooted and in the process of booting up, large quantities (about 16000) of the following error message appear on the standby RP console:

  ```
  service-policy VLAN_OUTPUT_POLICY can't be attached without corresponding
  service-fragment policy on appropriate target first
  ```

  The appearance of these error messages cannot be turned off, even with **no logging console** configured, and causes the standby RP boot up time to triple from its usual 15 to 20 minutes to more than 50 minutes.

  This condition occurs because in a Model 3 QoS configuration, the main interfaces must be attached before the fragment policy on the VLAN subinterfaces can be attached. Stopping or removing the SPA-8X1GE-V2 violates this requirement, resulting in the above error messages.

  There are no known workarounds.

- CSCsr97059

  When a Flexible Packet Matching (FPM) class is replaced with a similar class within the same parent policy on a Cisco ASR 1000 Series Router, the correct FPM action is not followed. Packets are still being allowed through the router; the expected action would be for packets to be dropped due to the drop action child policy.

The **show policy-map type access-control interface** output shows the FPM classification as correct.

Workaround: If you re-add the original class, the correct FPM action is followed.

- CSCsr97633

  External BGP (eBGP) neighbors on a Cisco ASR 1000 Series Router get stuck in the OpenSent state after an RP switchover until the hold-time expires.

  This condition causes traffic drop.

  There are no known workarounds.

- CSCsu05477

  The standby RP console on a Cisco ASR 1000 Series Router, which is disabled by default, may occasionally become enabled upon router boot-up. There is no functional impact on the system due to the standby console being enabled.

  There are no workarounds.

- CSCsu06783

  When using a scaled Policy Based Routing (PBR) configuration with a large number of subinterfaces and Border Gateway Protocol (BG)P sessions on a Cisco ASR 1000 Series Router, the BGP sessions go down.

  This condition is observed under the following scenario:

  – When a large PBR configuration (of several hundred route-maps) is used with a large number (several hundred) of subinterfaces.

  – When the IP virtual routing and forwarding (VRF) selection feature is also configured on the subinterfaces and route-map.

  – When a large number (several hundred) of BGP sessions are in use.

  There are no known workarounds.

- CSCsu10336

  A truncated core file with TEMP_IN_PROGRESS as part of the filename is created on the Cisco ASR 1000 Series Router when a critical process resets on the Embedded Services Processor (ESP) or RP.

  There are no known workarounds.

- CSCsu10406

  The following error message is generated when reloading the Embedded Services Processor (ESP) on a Cisco ASR 1004 Router with IPSec configured on the chassis:

  ```
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp: cpp_cp encountered an error1
  ```

  The IPSec tunnels come up as normal.

  There are no known workarounds.

- CSCsu18185

  When traffic classification (TC) is applied to a subscriber session on a Cisco ASR 1000 Series Router using an undefined access control list (ACL), the packet counters are not updated for Intelligent Services Gateway (ISG).

  Workaround: Define the ACLs explicitly instead of using an undefined ACL.

- CSCsu25738

  When reloading an Ethernet SPA immediately after performing an RP switchover on a Cisco ASR 1000 Series Router with a high availability (HA) setup and a redundant RP, the error message "%SYS-3-MGDTIMER: Previous timer has bad forward linkage" is displayed on the console. There is no functional impact due to this error message.

  There are no known workarounds.

- CSCsu27642

  When the RP on a Cisco ASR 1000 Series Router performs a high availability (HA) failover, IPv6 unicast traffic loss ranging from 5 to 30 seconds occurs for a small number of destinations. The length of the interruption is dependent on the **ipv6 nd reachable-time** value.

  This condition occurs under the following scenario:

  - The router is forwarding IPv6 packets to a large number of destinations.
  - The router has a very large number (several thousand) of neighbor discovery (ND) cache entries.
  - The router performs HA failover from the primary to the secondary.

  Workaround: Set the **ipv6 nd reachable-time** value to ten minutes or longer.

  Further Problem Description: The traffic interruption is caused by the IPv6 ND refreshing cache entries using Neighbor Unreachability Detection (NUD) during HA failover convergence. If the ND has a very large cache then the additional load of NUD during the convergence period can cause some cache refreshes to fail, which results in the traffic interruption.

- CSCsu27824

  On a Cisco ASR 1000 Series Router, multicast packet loss of about 10 to 20 seconds may be observed under certain conditions about three minutes after an RP switchover.

  This condition occurs when the router has approximately 2000 (S,G) entries, each of which is associated with two outgoing interfaces (OIFs). The loss does not occur across all (S,G) entries in the system, but only a subset, and the router recovers within 10 to 20 seconds.

  Workaround: Configure the ip multicast redundancy nsf holdtime to be 60 seconds.

- CSCsu27878

  The Embedded Services Processor (ESP) of a Cisco ASR 1000 Series Router continually loses roughly 500 kilobytes of memory every 24 hours.

  There are no known workarounds.

  Further Problem Description: Software automatically runs in the background on an ongoing basis to collect and manage traffic statistics accumulated in the ESP's QuantumFlow Processor. This software fails to recycle a few bytes of its memory after each statistics collection. The failure to recycle memory does not affect the router functionality, including the QFP statistics. Under normal circumstances, the router has plenty of ESP free memory (presently, the largest deployed router configuration leaves around 700 MB of free memory), leaving several years' time before this leak exhausts all ESP free memory.

- CSCsu29303

  The following error message is observed on a Cisco ASR 1000 Series Router with a large configuration and PPP over Ethernet (PPPoE) configured:

  ```
  %EVENTLIB-3-TIMEHOG: F1: cpp_cp: undefined: 69405ms, Traceback= .....
  ```

  This message has no adverse impact on router functionality.

  There are no known workarounds.

- CSCsu33792

  When a Cisco ASR 1000 Series Router sends or receives traffic in the STALE state, the IPv6 neighbor state does not change to DELAY, PROBE, and then REACH as expected.

  This condition occurs when a cable is removed from and inserted into the GigabitEthernet interface; this condition does not occur when the interface is **shut/no shut**.

  Workaround: Configure a static **ipv6 neighbor** configuration.

- CSCsu35558

  Performing an SNMP walk on the CISCO-IETF-NAT-MIB on a Cisco ASR 1000 Series Router may cause an Embedded Services Processor (ESP) reload on both the active and standby ESPs.

  There are no known workarounds.

- CSCsu35640

  The RP on a Cisco ASR 1000 Series Router resets with following traceback when the **ip pim send-rp-discovery** command is unconfigured in global configuration mode:

  ```
  ASR1000-WATCHDOG: Process = Exec
  ```

  This condition occurs when the router is configured for PPP Terminated Aggregation (PTA) and per session multicast traffic, and 4K or 8K PPP over Ethernet (PPPoE) sessions are up.

  Workaround: Do not unconfigure the **ip pim send-rp-discovery** command in global configuration mode when 4K or 8K PPPoE sessions are up.

- CSCsu39895

  The IOSd process resets on the active RP on a Cisco ASR 1000 Series Router when the RP is running IPv4/6 unicast and IPv6 multicast traffic. The following error message is observed in the crashinfo file:

  ```
  000219: Sep 2 04:21:58.350 EDT: %SYS-2-MALLOCFAIL: Memory allocation of 1128 bytes
  failed from 0x124D2F64, alignment 0
  Pool: Processor Free: 449920 Cause: Memory fragmentation
  Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "ASR1000-RP Punt
  Service Process", ipl= 0, pid= 71
  -Traceback= 1#106b90f504fce8544ce4979667ec2d5d :10000000+50BF84 :10000000+50A19C
  :10000000+50A46C :10000000+15399A4 :10000000+153F834 :10000000+153FE34
  :10000000+24D2F68 :10000000+24D371C :10000000+24D3FC4 :10000000+24D21DC
  :10000000+8DF4B0 :10000000+8DFDB4 :10000000+8E022C :10000000+8E0298 :10000000+8D6030
  :10000000+265E11C
  ```

  There are no known workarounds.

- CSCsu41375

  The following **show infrastructure punt** commands are not generating output or their output hangs on a Cisco ASR 1000 Series Router:

  - **show platform hardware cpp active infrastructure punt config cause**
  - **show platform hardware cpp active infrastructure punt statistics type inject-drop**
  - **show platform hardware cpp active infrastructure punt statistics type global-drop**

  This condition occurs when continuous traffic is sent on a 10-port Gigabit Ethernet SPA for an extended interval or when the 10-Gbps Cisco ASR 1000 Series ESP (ASR1000-ESP10) is oversubscribed.

  There are no known workarounds.

- CSCsu41444

  A watchdog reset occurs in the Punt Service Process of a Cisco ASR 1000 Series Router.

  This condition was observed in a configuration with 400K VPNv4 prefixes over 1K virtual routing and forwarding (VRF) instances without any traffic.

  Workaround: Reduce the number of VRFs and prefixes.

- CSCsu42105

  The Cisco ASR 1000 Series Router does not re-mark the differentiated services code point (DSCP) for the following IPv6 neighbor discovery (ND) packets:

  – The Duplicate Address Detection (DAD) neighbor solicitation (NS) packet for the link local address

  – The neighbor advertisement (NA) (Frame 55) for the link local address after a link flap

  There are no known workarounds.

- CSCsu43290

  On a Cisco ASR 1000 Series Router, performing a start/stop of two SPAs at the same time with triple play traffic may cause the following traceback to appear at the console:

  ```
  %SYS-2-NOTQ: unqueue didn't find 3B8B8D64 in queue 1407A5C0 -Process= "
  CHKPT rcv MSG process", ipl= 2, pid= 80
  ```

  There is no functional impact due to this traceback.

  There are no known workarounds.

- CSCsu43408

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router continually loses roughly 500 kilobytes of memory every 24 hours.

  There are no known workarounds.

  Further Problem Description: Software automatically runs in the background on an ongoing basis to collect and manage traffic statistics accumulated in the ESP's QuantumFlow Processor. This software fails to recycle a few bytes of its memory after each statistics collection. The failure to recycle memory does not affect the router functionality, including the QFP statistics. Under normal circumstances, the router has plenty of ESP free memory (presently, the largest deployed router configuration leaves around 700 MB of free memory), leaving several years' time before this leak exhausts all ESP free memory.

- CSCsu44557

  On a Cisco ASR 1000 Series Router, the memory allocation for Border Gateway Protocol (BGP) processes on the RP increases after clearing BGP sessions. In addition, the BGP summary counter is also incorrectly incremented.

  There are no known workarounds.

- CSCsu45138

  On a Cisco ASR 1000 Series Router, the Service Control Engine (SCE) sends the wrong IP address in a session query request to the Intelligent Services Gateway (ISG).

  There are no known workarounds.

- CSCsu45307

  The number of sessions in the READY state on the standby RP of a Cisco ASR 1000 Series Router does not match the number of sessions in the READY state on the currently active RP.

  This condition occurs with 16K active sessions when both the Point-to-Point Protocol (PPP) and QoS are configured. If just PPP is configured, the problem does not occur.

  There are no known workarounds.

- CSCsu46027

  When a port-channel member link failure and an RP failover occur in close proximity, the Cisco ASR 1000 Series Router does not switch outgoing traffic from the failed member link to the secondary member link immediately. This condition can occasionally result in packet loss of more than 10 seconds for packets that used to be active on the failed link.

  This condition is observed on a router with 8000 VLAN subinterfaces across 8 port channels under the following scenario:

  - Each port channel has 1000 VLAN subinterfaces.
  - Each port-channel interface consists of two physical Gigabit Ethernet interfaces from two different SPAs.
  - Manual VLAN load-balancing is configured in which 500 VLAN subinterfaces are active on each of the member links and the other member link is the standby.

  There are no known workarounds.

- CSCsu46531

  On a Cisco ASR 1000 Series Router, the active RP CPU utilization spikes for 40 seconds, as the active RP works through the process of synchronizing a large customer configuration to the standby RP.

  There are no known workarounds.

- CSCsu47120

  When the Cisco ASR 1000 Series Router reloads several times, the **show facility-alarm status** command reports a CRITICAL Physical Port Link Down on a Gigabit Ethernet SPA.

  Workaround: Issue the **hw-module reload** command on the SPA to clear the alarm.

- CSCsu47716

  Point-to-Point Protocol (PPP) session disconnects occur on a Cisco ASR 1000 Series Router because of Link Control Protocol (LCP) negotiation failures. The sessions eventually do come up.

  There are no known workarounds.

- CSCsu48111

  When the CPU usage rate of the Cisco QuantumFlow Processor (QFP) on a Cisco ASR 1000 Series Router is high, the input policy-map counter is not incremented.

  This condition occurs under the following scenario:

  - Low flow
  - High PPS rate
  - Continuous traffic for 1 minute or more

  There are no known workarounds.

- CSCsu48364

  A QoS configuration does not get successfully installed in the Cisco QuantumFlow Processor (QFP) after an RP switchover on a Cisco ASR 1000 Series Router. Tracebacks of the following form are observed on the IOS console:

  ```
  FMFP-3-OBJ_DWNLD_TO_CPP_FAILED
  ```

  This condition occurs in scaled scenarios such as 16K sessions/8K tunnels with a Model D.2 QoS configuration.

  There are no known workarounds.

- CSCsu50406

  When a Cisco ASR 1000 Series Router is reloaded or an online insertion and removal (OIR) insertion is performed on one of its SPAs, an error message is generated and the QoS policy is suspended.

  This condition occurs when a QoS policy is attached to the Multilink PPP (MLP) bundle that has **shape %** *n* configured where *n* is less than 13.

  Workaround: Manually remove and then reattach the QoS policy to the MLP bundle.

- CSCsu50921

  When more than 500 IPSec sessions are brought up, cleared and then brought up again across a Dynamic Virtual Tunnel Interface (DVTI) and Easy VPN (EzVPN) setup on a Cisco ASR 1000 Series Router, the IPSec tunnels come up but traffic doesn't get through and Cisco QuantumFlow Processor (QFP) flows cease to exist.

  Workaround: Use dynamic crypto maps with EzVPN instead of Dynamic VTI.

- CSCsu53066

  A Cisco ASR 1000 Series Router may experience more than 100 millisecond turnaround times (TAT) or message response latencies for H.248 Session Border Controller (SBC) requests.

  QoS statistics collection and regular changes in the VLAN configuration can also contribute to the extended message response latencies.

  Workaround: Reduce the number of configured VLANs, turn off QoS statistics, and minimize the amount of VLAN configuration changes to help keep the message response latencies down. Message response latencies can also be minimized by issuing the **parser config cache interface** command and the **show running-config** command prior to allowing H.248 SBC requests into the system.

- CSCsu55070

  If **no cdp enable** is configured on a few ports on a POS-OC48 SPA and the Cisco ASR 1000 Series Router is reloaded, the Cisco Discovery Protocol (CDP) gets disabled on all the ports.

  This condition occurs when the configuration is saved prior to the reload.

  Workaround: Add **cdp enable** to the ports you do not want to have disabled prior to the reload.

- CSCsu59082

  Inserting Border Gateway Protocol (BGP) routes into a virtual routing and forwarding (VRF) instance resets the Cisco ASR 1000 Series Router, even if no MPLS-enabled interfaces present.

  Workaround: Upgrade to a more recent image and issue the **mpls label mode all-vrfs protocol all-afs per-vrf** command to configure one label for each VRF to lessen the load on the control plane. (By default the **per-prefix label allocation** is used, that is, one label for each prefix.)

- CSCsu61385

  On a Cisco ASR 1000 Series Router, Peripheral Interface Manager (PIM) state-refresh messages are not generated with a PIM dense mode configuration. As a result, pruned interfaces time out in the forwarding state.

  Workaround: Use PIM dense mode to support only the extremely low rate data traffic. Use PIM Source Specific Mode (SSM) or Sparse Mode to support high rate traffic.

- CSCsu64094

  On a Cisco ASR 1000 Series Router, Frame-Relay data-link connection identifier (DLCI) counters do not increment when more than 80 DLCIs are configured on a Frame Relay interface or subinterface.

  There are no known workarounds.

- CSCsu67138

  On a Cisco ASR 1000 Series Router, the **show ip local pool** command does not display the in use IP addresses when an L2TP Network Server (LNS) is configured with high availability (HA) and the **ip local pool** command is configured. As a result after a switchover, IP addresses are not allocated from the pool. This condition results in duplicate IP address assignments.

  There are no known workarounds.

- CSCsu67864

  After the end user replaces his home gateway (HGW) (the DHCP client) physically on a Cisco ASR 1000 Series Router configured as a Dynamic Host Configuration Protocol (DHCP) relay, the new HGW never receives the DHCP Offer from the router. This condition results in the failure of IPv4 address allocation on the newly replaced HGW.

  Workaround: As a temporary workaround, the router administrator can clear the Address Resolution Protocol (ARP) table.

- CSCsu91220

  The **show issu version detail** command fails on a Cisco ASR 1000 Series Router with the error "Error connecting to command relay server".

  This problem is observed when the **no ip subnet-zero** command is configured in the system startup configuration.

  Workaround: Remove the **no ip subnet-zero** configuration command from the startup configuration and reload the system.

Resolved Caveats—Cisco IOS XE Release 2.2.1

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.2.1.

- CSCsm27071

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload. Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml

Release 2.1 Caveats

Caveats describe unexpected behavior in Cisco IOS XE Release 2. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

This section contains open and resolved caveats for the current Cisco IOS XE maintenance release.

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://www.cisco.com/en/US/docs/internetworking/terms_acronyms/ita.html

This section consists of the following subsections:

Open Caveats—Cisco IOS XE Release 2.1.2

This section documents possible unexpected behavior by Cisco IOS XE Release 2.1.2

- CSCsm55507

  On a Cisco ASR 1000 Series Router, when the IP MTU on a Generic Routing Encapsulation (GRE) tunnel interface exceeds that on the physical interface carrying tunnel traffic, the traffic requiring fragmentation may be dropped over time.

  Workaround: Configure an IP MTU on the tunnel interface no greater than that on the physical interface carrying tunnel traffic.

- CSCsm98756

  CPU usage peaks at 99 percent for a sustained period when the **show run | inc ipv6 route** command is issued with a large-scale configuration (thousands of VLANs) on a Cisco ASR 1000 Series Router, and various control plane functions such as Session Border Controller (SBC) call setup may not function as expected.

  Workaround: Reduce the **show run** command output to a file for post-processing.

- CSCsq08067

  On a Cisco ASR 1000 Series Router, if the **nbar protocol-discovery** command is configured on multiple interfaces (for example, 200) using the **interface range** command, then the **nbar protocol-discovery** configuration is removed from all VLANs except the first VLAN after an RP switchover.

  This condition occurs after an RP switchover on the Cisco ASR 1006 Router, or an IOSd switchover on the Cisco ASR 1004 Router.

  Workaround: Instead of using the **interface range** command, configure the **nbar protocol-discovery** command for each interface individually.

- CSCsq22332

  After provisioning different name servers in the global IP view and within a VRF on a Cisco ASR 1000 Series Router, a ping to a host within the VRF uses the name server in the global space to attempt to resolve the hostname.

  This condition occurs because the ping application does not support VRF Domain Name System (DNS) resolution. The ping application need to be extended to support VRF-aware DNS resolution.

  There are no known workarounds.

- CSCsq25196

  Border Gateway Protocol (BGP) Non-Stop Forwarding Graceful Restart (NSF-GR) does not work in a scaled setup on a Cisco ASR 1000 Router Series if the convergence time is more than 10 minutes.

  There are no known workarounds.

- CSCsq35705

  The cbQosPoliceCfgTable is failing for some configurations on a Cisco ASR 1000 Series Router. When **confirm burst** and **exceed burst** are not configured explicitly, the cbQosPoliceCfgTable is not getting populated.

  Workaround: Configure **confirm burst** and **exceed burst** explicitly, and the cbQosPoliceCfgTable will get populated as expected.

- CSCsq37627

  When reloading a Cisco ASR 1000 Series Router with a crypto map definition applied to two interfaces, removing the crypto map definition (using the **no crypto map** command) from the primary interface may reset the ESP.

  Workaround: Apply the crypto map definition to the interfaces after the reload.

  Further Problem Description: This problem occurred after removing the crypto map definition from a tunnel interface, which happened to be the primary interface (first interface that is used in spd_if_bind_a() after a reload).

- CSCsq70140

  The following error message appears on the Cisco ASR 1002 Router and the Cisco ASR 1004 Router:

  ```
  No memory available: Update of NVRAM config failed!
  ```

  This message appears more frequently when the user is saving a very big configuration, such as a configuration with 16K interfaces on a Cisco ASR 1002 Router or Cisco ASR 1004 Router. This problem is not seen on the Cisco ASR 1006 Router.

  There are no known workarounds.

- CSCsq75133

  When Bidirectional Forwarding Detection (BFD) echo mode (the default mode) and Unicast Reverse Path Forwarding (uRPF) are both enabled on an interface on a Cisco ASR 1000 Series Router, traceback of bfd_get_bfd_idb is seen on the standby RP.

  Workaround: Disable echo mode on the interface using the **no bfd echo** command. For example:

  ```
  Router(config-if)# no bfd echo
  ```

- CSCsq77838

  A memory leak can occur in the QuantumFlow processor (QFP) datapath when the Cisco ASR 1000 Series Router has to reassemble fragmented IP packets over an IP tunnel at very high rates (of the order of 5Gbps or more.) When this condition occurs, the following error message is displayed on on the console:

  ```
  %MEM_MGR-3-MALLOC_NO_MEM: pool handle 0x8db00000, size 144
  ```

  Workaround: Avoid fragmentation on the IP tunnel router header so that the tunnel end point on the router does not need to perform reassembly by configuring the IP Maximum Transmission Unit (MTU) of the tunnel interface to be small enough so that the physical interface level does not need to fragment packets based on the physical interface's IP MTU.

- CSCsq90358

  On a Cisco ASR 1000 Series Router, the ESP may reload when 4K IPSec tunnels are configured with Internet Key Exchange (IKE) and IPSec lifetimes that are shorter than the default lifetimes. (The default IKE lifetime is 24 hours, and the default IPSec lifetime is 60 minutes.)

  Workaround: Either configure the IKE lifetime to be the default value (24 hours) or longer, and configure the IPSec lifetime to be the default value (60 minutes) or longer, or reduce the total number of tunnels to 2K. Future software upgrades may reduce this limitation.

- CSCsr00490

  On a Cisco ASR 1000 Series Router with random detect configured, if a policy map is attached to multiple interfaces/parent policies, each instance shares the same Weighted Random Early Detection (WRED) threshold information. This behavior is not a problem if all attachment points are the same speed. However, if the policy map is attached to attachment points of different speeds (such as two different interface types or parent policies), the WRED thresholds shared may be inappropriate for one or more instances and may lead to unexpected drop behavior.

  This condition occurs because the control plane calculates default WRED curves based on the interface bandwidth and currently only supports one curve per class per policy map.

  Workaround: Configure a unique policy map for each speed instance/interface type or parent policy that is required. In other words, if you have a policy map “p” applied to a Gigabit Ethernet interface, with random-detect applied, that policy map should only be applied to like interfaces. If you want to configure another interface type with the same policy map, you should create another policy map “p2”, which is identical to “p1” except in name, and apply that policy map to the new interface type.

- CSCsr01097

  New Skinny and H.323 protocol calls can not be made after a prolonged run of traffic with these protocols on a Cisco ASR 1000 Router.

  This condition occurs because memory consumption in the Cisco QuantumFlow processor (QFP) builds up, leaving no free space for new calls.

  Workaround: If you clear the calls using the **clear zone inspect session** command, you may be able to run traffic for a longer duration.

- CSCsr03480

  When a Cisco ASR 1006 Router with a redundant RP and a redundant ESP has a large running-config, the standby ESP can unexpectedly reload when additional configurations are added to the existing running-config. This condition has been seen with the following configuration:

  - 1K IPSec sessions (250 over POS/Frame-Relay, 750 over VLANs)
  - 1 MLPPP link with QoS
  - 2 VLANs with hierarchical QoS

  - 2K SIP/Skinny sessions
  - 250 GRE tunnels with NAT, NetFlow, OSPF, and RIP

  The reload occurred when 250 Gigabit Ethernet VLANs were added to the original configuration. It is possible that this condition may occur under other scenarios.

  There are no known workarounds.

- CSCsr22866

  Enhanced Interior Gateway Routing Protocol (EIGRP) Peer MIB information is missing from the EigrpPeerTable on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsr36498

  When the **bandwidth** command is applied to any Layer 3 and above physical interface on a Cisco ASR 1000 Series Router, the actual throughput of the physical interface gets changed.

  There are no known workarounds.

- CSCsr51882

  The ESP on a Cisco ASR 1000 Series Router resets when a service policy is removed from the VIF and CTunnel interfaces.

  Workaround: Disable quality of service (QoS) commands on the VIF and CTunnel interfaces. QoS is not supported on these interfaces.

- CSCsr53669

  The forward packet counter displayed by the **show ipv6 traffic** command on a Cisco ASR 1000 Series Router is incremented when an IPv6 ICMP packet is generated by the RP. This forward counter should only be incremented when a packet is forwarded by the router.

  There are no known workarounds.

- CSCsr56775

  On a Cisco ASR 1000 Series Router with Hierarchical QoS applied, if a policer is configured on the parent and child policies, no **shape** or **bandwidth** commands are configured, and then the child policy is removed, the parent policy will not be applied.

  There are no known workarounds.

- CSCsr60513

  When a class and shape average are configured for the same class on a Cisco ASR 1000 Series Router, the Weighted Random Early Detection (WRED) counters are not updated after enabling Explicit Congestion Notification (ECN).

  There are no known workarounds.

- CSCsr66075

  A Cisco ASR 1000 Series Router running an FRF.12 configuration returns the following error:

  ```
  Jul 30 14:07:03.736 EST: %SPA_CHOC_DSX-3-HDLC_CTRL_ERR: SIP2/0: SPA 2/0: 5 TX Chnl
  Queue Overflow events on HDLC Controller were encountered
  ```

  In addition to this message, packets are dropped.

  This condition is observed on FR interfaces where a large percentage of the traffic being sent is fragmented, but which also experience periods of non-fragmented (priority) traffic.

  Workaround: No workaround is required. The message is an indication that packets have been dropped due to an overrun condition. The router will self recover.

- CSCsr87300

  When an ESP switchover is performed on a Cisco ASR 1000 Series Router, resets may occur during the initialization of the new standby ESP.

  This condition is only observed with broadband configurations when ESP1 is the active ESP before the switchover.

  There are no known workarounds.

- CSCsr93102

  A Copper GE interface on a Cisco ASR 1000 Series Router goes down after a router reload.

  This condition occurs when the interface speed is configured as 100Mbps and auto-negotiation is disabled. After the reload, the interface configuration is not getting re-applied. As a result, the link-protocol goes down.

  Workaround: Perform a **shut/no shut** of the interface to bring back the link.

- CSCsr94078

  The presence of Border Gateway Protocol (BGP) routes on a Cisco ASR 1000 Series Router may increase the time for the Interior Gateway Protocol (IGP) (ISIS or OSPF) to converge and update the forwarding table following a network failure.

  This condition occurs if the outgoing interface to the nexthop of the BGP prefixes is changed due to the convergence.

  There are no known workarounds.

  Further Problem Description: The magnitude of the convergence time increase is probably dependant on the number of BGP routes.

- CSCsr95180

  The **show platform hardware** command output is incorrect for some IPv4 routes on a Cisco ASR 1000 Series Router.

  This condition occurs when IPv4 multicast is configured, the **show platform hardware** command is executed for the multicast prefix, and the prefix has ".0" at the end (for example, 225.3.2.0/32).

  There are no known workarounds.

- CSCsr99022

  When a virtual-template interface is removed and then re-configured on a Cisco ASR 1000 Series Router, the system fails to create the virtual-template interface.

  Workaround: Do not remove the virtual-template interface.

- CSCsu01606

  A Border Gateway Protocol (BGP) PE-PE session on a Cisco ASR 1000 Series Router gets stuck in the closing state for 5-10 minutes after the core link is shut.

  This condition was observed on a l3 VPN setup with BGP multipath configured that included 2 Interior Gateway Protocol (IGP) equal cost paths in the core.

  There are no known workarounds.

- CSCsu05743

  When performing an In Service Software Upgrade (ISSU) between any two versions of Cisco IOS XE Release 2.1.0, 2.1.1, and 2.1.2 on a Cisco ASR 1000 Series Router, firewall sessions are not synchronized to the standby ESP after ISSU. As a result, the following error message might be reported by the active ESP (F0 in the example below):

  ```
  Sep 11 02:26:03.407 PDT: %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00  Thread:080 TS:00000
  001589974161890 %FWALL-3-HA_INVALID_MSG_RCVD: invalid version 65539 opcode b -Trac
  eback= 801e9f58 800fd87c 800d9489
  ```

  There are no known workarounds; this condition is benign.

- CSCsu13500

  The ESP on a Cisco ASR 1000 Series Router unexpectedly reloads when a NetFlow exporter configuration is removed.

  This condition is observed in scenarios with multiple exporters, at least one of which is v9.

  Workaround: Do not remove NetFlow v9 exporter configurations on running systems.

- CSCsu35829

  On a Cisco ASR 1000 Series Router, the fman_rp process reloads and some PPPoE sessions go down and back up again.

  This condition was observed when executing snmp query, copy image, IOS commands and RP commands with 4000 PPPoE sessions and bi-directional traffic.

  There are no known workarounds.

- CSCsu38228

  On a Cisco ASR 1000 Series Router with Weighted Random Early Detection (WRED) enabled, when **random-detect exponential-weighting-constant** is reset with valid values (1-6, default is 4) and removed from the policy-map applied, the random-detect exponential-weighting-constant is set to 9.

  Workaround: Reconfigure **random-detect exponential-weighting-constant** to the correct value.

- CSCsu68057

  On a Cisco ASR 1000 Series Router, an IOSd reset occurs while running an automated script that executes the **no cns config initial** command when the primary interface out of the device is shutdown. When the **no cns config initial** command is executed manually, no reset is observed.

  Workaround: Instead of using the **no cns config partial** command in the script, use the following complete command:

  no cns config initial {*ip-address* | *host-name*} [**encrypt**] [*port-number*] [**page** *page*] [**syntax-check**] [**no-persist**] [**source** *ip-address*] [**status** *url*] [**event**] [**inventory**]

- CSCsu75596

  The ESP on a Cisco ASR 1000 Series Router may reload if a neighboring interface configured with Open Shortest Path First (OSPF) over Generic Routing Encapsulation (GRE)/Frame Relay (FR) goes down.

  This condition occurs when the **shutdown** command is executed on a serial subinterface used for GRE and OSPF.

  Workaround: Remove the OSPF configuration and stop traffic while performing this action.

- CSCsu91220

  The **show issu version detail** command fails on a Cisco ASR 1000 Series Router with the error "Error connecting to command relay server".

  This problem is observed when the **no ip subnet-zero** command is configured in the system startup configuration.

  Workaround: Remove the **no ip subnet-zero** configuration command from the startup configuration and reload the system.

Resolved Caveats—Cisco IOS XE Release 2.1.2

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.1.2.

- CSCsl49274

  A Cisco ASR 1000 Series Router may reset when the **show interface random-detect** command is executed.

  This condition occurs only when a policy map is configured with Weighted Random Early Detection (WRED) in the class-default class, and the policy map is applied to an interface.

  Workaround: Use the **show policy-map interface** command instead of the **show interface random-detect** command.

  Further Problem Description: The **show interface random-detect** command is a legacy QoS command and is not supported on the Cisco ASR 1000 Series Router.

- CSCsm49243

  On a Cisco ASR 1000 Series Router, **ip dhcp relay** commands (**ip dhcp relay information option server-id-override** and **ip dhcp relay source-interface Loopback0**) configured under interface range may not synchronize over to the newly active Route Processor (RP) after switchover.

  Workaround: Instead of using range commands, configure the interfaces individually.

- CSCso38119

  On a Cisco ASR 1000 Series Router, when control plane changes are made to Quality of Service (QoS), or subinterfaces are added that have a service policy applied when the physical interface associated with the control plane changes is over-subscribed, the following error message is reported on the console:

  ```
  CPPBQS-3-QMOVEFAIL: F0: cpp_cp: CPP 0 schedule InterfaceSchedule queue move failed
  (0xa6090402) - SEID=0x141 SID=0X280C1
  ```

  This severe condition will prohibit further configuration changes and cause inconsistencies between the control plane and data plane.

  Workaround: Avoid making control plane changes involving QoS when the physical interface associated with the changes is over-subscribed.

- CSCso71857

  A Packet-over-SONET (POS) SPA on the Cisco ASR 1000 Series Router incorrectly reports a line alarm indication signal (LAIS) alarm as a Section Bit Interleaved Parity alarm and issues the following error message:

  ```
  *Apr 9 11:09:47: %ASR1000_RP_SONET_ALARM-6-POS: ASSERT CRITICAL POS0/2/1 Section Bit
  Interleaved Parity
  ```

  There are no known workarounds.

- CSCso73923

  On a Cisco ASR 1000 Series Router, an unexpected reload of the Embedded Services Processor (ESP) may be seen if fair-queue is added to or deleted from an existing policy-map.

  This reload has been observed when a hierarchical Quality of Service (QoS) policy was modified to apply the **fair-queue** command as part of the existing child policy.

  Workaround: Detach the service-policy prior to modification, then re-attach the service-policy back to the interface.

- CSCsq08697

  The following error messages are seen on the RP console of a Cisco ASR 1000 Series Router during router boot up after upgrading from Cisco IOS XE Release 2.0 to Cisco IOS XE Release 2.1:

```
plim qos input map ip dscp  32  queue low-latency
% Invalid input detected at '^' marker
plim qos input map ipv6 tc  32  queue low-latency
% Invalid input detected at '^' marker
```

  This condition occurs because in the Cisco IOS XE Release 2.0 release of Cisco ASR 1000 software, the high priority queue for the physical layer interface module (PLIM) QoS at the input of an interface is configured using the using the **low-latency** keyword as shown below:

```
Router(config-if)# plim qos input queue ?
0            Low priority queue
low-latency  High priority queue
Router(config-if)#
Router(config-if)# plim qos input map ip dscp ef queue ?
0            Low priority queue
low-latency  High priority queue
Router(config-if)#
Router(config-if)# plim qos input map ipv6 tc ef queue ?
0            Low priority queue
low-latency  High priority queue
Router(config-if)#
```

  In contrast, beginning with Cisco IOS XE Release 2.1, the high priority queue for PLIM QoS at the input of an interface is configured using **strict-priority** keyword as shown below:

```
Router(config-if)# plim qos input queue ?
0                Low priority queue
strict-priority  High priority queue
Router(config-if)#
Router(config-if)# plim qos input map ip dscp ef queue ?
0                Low priority queue
strict-priority  High priority queue
Router(config-if)#
Router(config-if)# plim qos input map ipv6 tc ef queue ?
0                Low priority queue
strict-priority  High priority queue
Router(config-if)#
```

  Workaround: Reconfigure the PLIM QoS input map for an interface after the software upgrade using the **strict-priority** keyword instead of the **low-latency** keyword, and save the new configuration.

- CSCsq11427

  If Point-to-Point Protocol (PPP) authorization is in use on a Cisco ASR 1000 Series Router, a small amount of memory leaks for each PPP connection processed by the router.

  There are no known workarounds.

- CSCsq72274

  On a Cisco ASR 1000 Router, the audio port information (in the SDP) may not be translated correctly for an inside-to-side call with a Port Address Translation (PAT) or an interface overload Network Address Translation (NAT) configuration.

  There are no known workarounds.

- CSCsq77500

  The MEM_MGR-3-MALLOC_NO_MEM message appears on the console of a Cisco ASR 1000 Series Router.

  This condition occurs because the IP packet passing through the generic routing encapsulation (GRE) tunnel is bigger in size than the IP Maximum Transmission Unit (MTU) defined for that tunnel interface. If IP fragmentation continues for the GRE tunnel, eventually ESP memory will be used up.

  There are no known workarounds.

- CSCsq79348

  When a Cisco ASR 1000 Series Router is running IPSec with Network Address Translation (NAT), the following message may appear on the standby ESP when the IPSec session is created:

  ```
  CPP-NAT:NAT-3-HA_COULD_NOT_FIND_SESS
  ```

  This message indicates that not all the IPSec data was transferred properly to the standby ESP. As a result, if a switchover occurs, the corresponding IPSec sessions will have to be reestablished.

  There are no known workarounds.

- CSCsq87265

  A Cisco ASR 1000 Series Router may experience an unexpected system reload during L2TP Network Server (LNS) session establishment.

  This condition can occur on a router that is configured as an L2TP Network Server (LNS) when the subscriber IP address overlaps with a tunnel peer IP address as in the following example:

  ```
  Router(config)# interface TenGigabitEthernet0/2/0
  Router(config-if)# ip address 10.20.20.1 255.255.0.0
  Router(config-if)# exit
  Router(config)# interface Virtual-Template 1
  Router(config-if)# peer default ip address pool default
  Router(config-if) #exit
  Router(config)# ip local pool default 10.20.20.2 10.20.20.254
  ```

  Workaround: Configure the subscriber address pool so that it does not overlap with the tunnel peer IP address.

- CSCsq96258

  The Embedded Services Processor (ESP) software on a Cisco ASR 1000 Series Router may reload with a series of memory messages after a route processor (RP) switchover event.

  This condition can occur occasionally when the system is configured with a total of 500K prefixes, 1K VRFs, and 1K eBGP sessions during an RP switchover.

  Workaround: Reduce the number of prefixes (or routes) to below 500K.

Open Caveats—Cisco IOS XE Release 2.1.1

This section documents possible unexpected behavior by Cisco IOS XE Release 2.1.1

- CSCsl49274

  A Cisco ASR 1000 Series Router may reset when the **show interface random-detect** command is executed.

  This condition occurs only when a policy map is configured with Weighted Random Early Detection (WRED) in the class-default class, and the policy map is applied to an interface.

  Workaround: Use the **show policy-map interface** command instead of the **show interface random-detect** command.

  Further Problem Description: The **show interface random-detect** command is a legacy QoS command and is not supported on the Cisco ASR 1000 Series Router.

- CSCsm49243

  On a Cisco ASR 1000 Series Router, **ip dhcp relay** commands (**ip dhcp relay information option server-id-override** and **ip dhcp relay source-interface Loopback0**) configured under interface range may not synchronize over to the newly active route processor (RP) after switchover.

  Workaround: Instead of using range commands, configure the interfaces individually.

- CSCsm55507

  On a Cisco ASR 1000 Series Router, when the IP MTU on a Generic Routing Encapsulation (GRE) tunnel interface exceeds that on the physical interface carrying tunnel traffic, the traffic requiring fragmentation may be dropped over time.

  Workaround: Configure an IP MTU on the tunnel interface no greater than that on the physical interface carrying tunnel traffic.

- CSCsm98756

  CPU usage peaks at 99 percent for a sustained period when the **show run | inc ipv6 route** command is issued with a large-scale configuration (thousands of VLANs) on a Cisco ASR 1000 Series Router, and various control plane functions such as Session Border Controller (SBC) call setup may not function as expected.

  Workaround: Reduce the **show run** command output to a file for post-processing.

- CSCso38119

  On a Cisco ASR 1000 Series Router, when control plane changes are made to Quality of Service (QoS), or subinterfaces are added that have a service policy applied when the physical interface associated with the control plane changes is over-subscribed, the following error message is reported on the console:

  ```
  CPPBQS-3-QMOVEFAIL: F0: cpp_cp: CPP 0 schedule InterfaceSchedule queue move failed
  (0xa6090402) - SEID=0x141 SID=0X280C1
  ```

  This severe condition will prohibit further configuration changes and cause inconsistencies between the control plane and data plane.

  Workaround: Avoid making control plane changes involving QoS when the physical interface associated with the changes is over-subscribed.

- CSCso61824

  Under rare conditions, a SPA fails to come online when the Cisco ASR 1000 Series Router is reloaded when the Route Processor (RP) is busy processing a large configuration. The SPA process experiences multiple resets.

  Workaround: To recover from the SPA failure condition, reload the SIP.

- CSCso71857

  A Packet-over-SONET (POS) SPA on the Cisco ASR 1000 Series Router incorrectly reports a line alarm indication signal (LAIS) alarm as a Section Bit Interleaved Parity alarm and issues the following error message:

  ```
  *Apr 9 11:09:47: %ASR1000_RP_SONET_ALARM-6-POS: ASSERT CRITICAL POS0/2/1 Section Bit
  Interleaved Parity
  ```

  There are no known workarounds.

- CSCso73923

  On a Cisco ASR 1000 Series Router, an unexpected reload of the Embedded Services Processor (ESP) may be seen if fair-queue is added to or deleted from an existing policy-map.

  This reload has been observed when a hierarchical Quality of Service (QoS) policy was modified to apply the **fair-queue** command as part of the existing child policy.

  Workaround: Detach the service-policy prior to modification, then re-attach the service-policy back to the interface.

- CSCsq08067

  On a Cisco ASR 1000 Series Router, if the **nbar protocol-discovery** command is configured on multiple interfaces (for example, 200) using the **interface range** command, then the **nbar protocol-discovery** configuration is removed from all VLANs except the first VLAN after an RP switchover.

  This condition occurs after an RP switchover on the Cisco ASR 1006 Router, or an IOSd switchover on the Cisco ASR 1004 Router.

  Workaround: Instead of using the **interface range** command, configure the **nbar protocol-discovery** command for each interface individually.

- CSCsq08697

  The following error messages are seen on the RP console of a Cisco ASR 1000 Series Router during router boot up after upgrading from Cisco IOS XE Release 2.0 to Cisco IOS XE Release 2.1:

  ```
  plim qos input map ip dscp  32  queue low-latency
  % Invalid input detected at '^' marker
  plim qos input map ipv6 tc  32  queue low-latency
  % Invalid input detected at '^' marker
  ```

  This condition occurs because in the Cisco IOS XE Release 2.0 release of Cisco ASR 1000 software, the high priority queue for the physical layer interface module (PLIM) QoS at the input of an interface is configured using the using the **low-latency** keyword as shown below:

  ```
  Router(config-if)# plim qos input queue ?
  0            Low priority queue
  low-latency  High priority queue
  Router(config-if)#
  Router(config-if)# plim qos input map ip dscp ef queue ?
  0            Low priority queue
  low-latency  High priority queue
  Router(config-if)#
  Router(config-if)# plim qos input map ipv6 tc ef queue ?
  ```

```
0            Low priority queue
low-latency  High priority queue
Router(config-if)#
```

In contrast, beginning with Cisco IOS XE Release 2.1, the high priority queue for PLIM QoS at the input of an interface is configured using **strict-priority** keyword as shown below:

```
Router(config-if)# plim qos input queue ?
0               Low priority queue
strict-priority  High priority queue
Router(config-if)#
Router(config-if)# plim qos input map ip dscp ef queue ?
0               Low priority queue
strict-priority  High priority queue
Router(config-if)#
Router(config-if)# plim qos input map ipv6 tc ef queue ?
0               Low priority queue
strict-priority  High priority queue
Router(config-if)#
```

Workaround: Reconfigure the PLIM QoS input map for an interface after the software upgrade using the **strict-priority** keyword instead of the **low-latency** keyword, and save the new configuration.

- CSCsq11013

  The **show ip route vrf** command shows active VPN routes for Border Gateway Protocol (BGP) sessions that are in the “Idle” state.

  There are no known workarounds.

- CSCsq11427

  If Point-to-Point Protocol (PPP) authorization is in use on a Cisco ASR 1000 Series Router, a small amount of memory leaks for each PPP connection processed by the router.

  There are no known workarounds.

- CSCsq22332

  After provisioning different name servers in the global IP view and within a virtual routing and forwarding (VRF) instance on a Cisco ASR 1000 Series Router, a ping to a host within the VRF uses the name server in the global space to attempt to resolve the hostname.

  This condition occurs because the ping application does not support VRF Domain Name System (DNS) resolution. The ping application need to be extended to support VRF-aware DNS resolution.

  There are no known workarounds.

- CSCsq25196

  Border Gateway Protocol (BGP) Non-Stop Forwarding Graceful Restart (NSF-GR) does not work in a scaled setup on a Cisco ASR 1000 Router Series if the convergence time is more than 10 minutes.

  There are no known workarounds.

- CSCsq35705

  The cbQosPoliceCfgTable is failing for some configurations on a Cisco ASR 1000 Series Router. When **confirm burst** and **exceed burst** are not configured explicitly, the cbQosPoliceCfgTable is not getting populated.

  Workaround: Configure **confirm burst** and **exceed burst** explicitly, and the cbQosPoliceCfgTable will get populated as expected.

- CSCsq37627

  When reloading a Cisco ASR 1000 Series Router with a crypto map definition applied to two interfaces, removing the crypto map definition (using the **no crypto map** command) from the primary interface may reset the ESP.

  Workaround: Apply the crypto map definition to the interfaces after the reload.

  Further Problem Description: This problem occurred after removing the crypto map definition from a tunnel interface, which happened to be the primary interface (first interface that is used in spd_if_bind_a() after a reload).

- CSCsq41016

  When an ESP switchover occurs during the time in which an IPSec Dynamic Virtual Tunnel Interface (DVTI) tunnel is being built on a Cisco ASR 1006 Router, many existing tunnels and all new tunnels will stop forwarding traffic.

  Workaround: Use a dynamic crypto map instead of DVTI.

- CSCsq70140

  The following error message appears on the Cisco ASR 1002 Router and the Cisco ASR 1004 Router:

  ```
  No memory available: Update of NVRAM config failed!
  ```

  This message appears more frequently when the user is saving a very big configuration, such as a configuration with 16K interfaces on a Cisco ASR 1002 Router or Cisco ASR 1004 Router. This problem is not seen on the Cisco ASR 1006 Router.

  There are no known workarounds.

- CSCsq72274

  On a Cisco ASR 1000 Router, the audio port information (in the SDP) may not be translated correctly for an inside-to-side call with a Port Address Translation (PAT) or an interface overload Network Address Translation (NAT) configuration.

  There are no known workarounds.

- CSCsq75133

  When Bidirectional Forwarding Detection (BFD) echo mode (the default mode) and Unicast Reverse Path Forwarding (uRPF) are both enabled on an interface on a Cisco ASR 1000 Series Router, traceback of bfd_get_bfd_idb is seen on the standby RP.

  Workaround: Disable echo mode on the interface using the **no bfd echo** command. For example:

  ```
  Router(config-if)# no bfd echo
  ```

- CSCsq77500

  The MEM_MGR-3-MALLOC_NO_MEM message appears on the console of a Cisco ASR 1000 Series Router.

  This condition occurs because the IP packet passing through the generic routing encapsulation (GRE) tunnel is bigger in size than the IP Maximum Transmission Unit (MTU) defined for that tunnel interface. If IP fragmentation continues for the GRE tunnel, eventually ESP memory will be used up.

  There are no known workarounds.

- CSCsq77838

  A memory leak can occur in the Cisco QuantumFlow processor (QFP) datapath when the Cisco ASR 1000 Series Router has to reassemble fragmented IP packets over an IP tunnel at very high rates (of the order of 5Gbps or more.) When this condition occurs, the following error message is displayed on the console:

  ```
  %MEM_MGR-3-MALLOC_NO_MEM: pool handle 0x8db00000, size 144
  ```

  Workaround: Avoid fragmentation on the IP tunnel router header so that the tunnel end point on the router does not need to perform reassembly by configuring the IP Maximum Transmission Unit (MTU) of the tunnel interface to be small enough so that the physical interface level does not need to fragment packets based on the physical interface's IP MTU.

- CSCsq79348

  When a Cisco ASR 1000 Series Router is running IPSec with Network Address Translation (NAT), the following message may appear on the standby ESP when the IPSec session is created:

  ```
  CPP-NAT:NAT-3-HA_COULD_NOT_FIND_SESS
  ```

  This message indicates that not all the IPSec data was transferred properly to the standby ESP. As a result, if a switchover occurs, the corresponding IPSec sessions will have to be reestablished.

  There are no known workarounds.

- CSCsq81270

  Open Shortest Path First (OSPF) adjacency is not established on a Cisco ASR 1000 Series Router with a point-to-multipoint broadcast network.

  There are no known workarounds.

- CSCsq87265

  A Cisco ASR 1000 Series Router may experience an unexpected system reload during L2TP Network Server (LNS) session establishment.

  This condition can occur on a router that is configured as an L2TP Network Server (LNS) when the subscriber IP address overlaps with a tunnel peer IP address as in the following example:

  ```
  Router(config)# interface TenGigabitEthernet0/2/0
  Router(config-if)# ip address 10.20.20.1 255.255.0.0
  Router(config-if)# exit
  Router(config)# interface Virtual-Template 1
  Router(config-if)# peer default ip address pool default
  Router(config-if) #exit
  Router(config)# ip local pool default 10.20.20.2 10.20.20.254
  ```

  Workaround: Configure the subscriber address pool so that it does not overlap with the tunnel peer IP address.

- CSCsq90358

  On a Cisco ASR 1000 Series Router, the ESP may reload when 4K IPSec tunnels are configured with Internet Key Exchange (IKE) and IPSec lifetimes that are shorter than the default lifetimes. (The default IKE lifetime is 24 hours, and the default IPSec lifetime is 60 minutes.)

  Workaround: Either configure the IKE lifetime to be the default value (24 hours) or longer, and configure the IPSec lifetime to be the default value (60 minutes) or longer, or reduce the total number of tunnels to 2K. Future software upgrades may reduce this limitation.

- CSCsq96258

  The ESP software on a Cisco ASR 1000 Series Router may reload with a series of memory messages after an RP switchover event.

  This condition can occur occasionally when the system is configured with a total of 500K prefixes, 1K VRFs, and 1K eBGP sessions during an RP switchover.

  Workaround: Reduce the number of prefixes (or routes) to below 500K.

- CSCsr00490

  On a Cisco ASR 1000 Series Router with random detect configured, if a policy map is attached to multiple interfaces/parent policies, each instance shares the same Weighted Random Early Detection (WRED) threshold information. This behavior is not a problem if all attachment points are the same speed. However, if the policy map is attached to attachment points of different speeds (such as two different interface types or parent policies), the WRED thresholds shared may be inappropriate for one or more instances and may lead to unexpected drop behavior.

  This condition occurs because the control plane calculates default WRED curves based on the interface bandwidth and currently only supports one curve per class per policy map.

  Workaround: Configure a unique policy map for each speed instance/interface type or parent policy that is required. In other words, if you have a policy map “p” applied to a Gigabit Ethernet interface, with random-detect applied, that policy map should only be applied to like interfaces. If you want to configure another interface type with the same policy map, you should create another policy map “p2”, which is identical to “p1” except in name, and apply that policy map to the new interface type.

- CSCsr01097

  New Skinny and H.323 protocol calls can not be made after a prolonged run of traffic with these protocols on a Cisco ASR 1000 Router.

  This condition occurs because memory consumption in the Cisco QuantumFlow processor (QFP) builds up, leaving no free space for new calls.

  Workaround: If you clear the calls using the **clear zone inspect session** command, you may be able to run traffic for a longer duration.

- CSCsr03480

  When a Cisco ASR 1006 Router with a redundant RP and a redundant ESP has a large running-config, the standby ESP can unexpectedly reload when additional configurations are added to the existing running-config. This condition has been seen with the following configuration:

  - 1K IPSec sessions (250 over POS/Frame-Relay, 750 over VLANs)
  - 1 Multilink PPP(MLPPP) link with QoS
  - 2 VLANs with hierarchical QoS
  - 2K SIP/Skinny sessions
  - 250 GRE tunnels with NAT, NetFlow, OSPF, and RIP

  The reload occurred when 250 Gigabit Ethernet VLANs were added to the original configuration. It is possible that this condition may occur under other scenarios.

  There are no known workarounds.

  Further Problem Description: This problem occurs because after an RP failover, the AOM object under fman-fp, takes up more memory than it had previously. There is no leak, and the memory will not increase on subsequent failovers. The increase only occurs during the first failover. If your configuration is already approaching the maximum memory available on the ESP, you might run into this issue on RP failover.

- CSCsu05743

  When performing an In Service Software Upgrade (ISSU) between any two versions of Cisco IOS XE Release 2.1.0 and 2.1.1 on a Cisco ASR 1000 Series Router, firewall sessions are not synchronized to the standby ESP after ISSU. As a result, the following error message might be reported by the active ESP (F0 in the example below):

  ```
  Sep 11 02:26:03.407 PDT: %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00  Thread:080 TS:00000
  001589974161890 %FWALL-3-HA_INVALID_MSG_RCVD: invalid version 65539 opcode b -Trac
  eback= 801e9f58 800fd87c 800d9489
  ```

  There are no known workarounds; this condition is benign.

Resolved Caveats—Cisco IOS XE Release 2.1.1

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.1.1.

- CSCsm05024

  After running traffic for an extended period of time on a Cisco ASR 1000 Series Router, a Route Processor (RP) switchover may result in a reload of the new standby RP when the RP attempts to synchronize the configuration.

  After an auto-reload, the standby RP again functions as expected.

  There are no known workarounds.

- CSCsm74141

  On a Cisco ASR 1000 Series Router, successive copying of qos configuration including issuing the **match access-group** command to the running configuration leads to duplicate entries for the match access-group clause.

  Workaround: This issue is strictly a **show configuration** issue and has no functional impact.

- CSCso16581

  The TIE on line interfaces that use network clocking, such as OC3 and OC12, can oscillate and fail to meet the 100 second settling time requirement.

  This condition can occur when the network clock input (the source of timing distribution for the box) undergoes rapid changes in frequency offset. Note that this is a rare and unusual condition but still permissible. A 10 PPM delta (+5 to -5 PPM) across 10 seconds can result in a failure to meet the TIE in this case.

  Workaround: The problem can be mitigated by ensuring that there is no rapid frequency offset change on the reference clock. There is no full workaround.

- CSCso77028

  On Packet-over-SONET (POS) interfaces on a Cisco ASR 1000 Series Router with Network Based Application Recognition (NBAR) configured (Protocol discovery and/or service policies), changing the NBAR configuration, then repetitively adding and/or removing NetFlow may cause the Embedded Services Processor (ESP) to reload. The reload may occur during or after the point at which NetFlow is enabled or disabled.

  Workaround: When NBAR and NetFlow are configured on a POS interface, allow a delay of 30 seconds or more between removing the NBAR configuration and the configuration/de-configuration of NetFlow.

- CSCso81177

  On a Cisco ASR 1000 Series Router, if Network Address Translation (NAT) is configured immediately after Network Based Application Recognition (NBAR) is de-configured, an unpredictable internal state can result.

  Workaround: Configure NAT before de-configuring NBAR, or wait until all NBAR links are removed or expired.

- CSCso83252

  Connecting multiple IPSec tunnels at the same time or in quick succession using a Dynamic Virtual Tunnel Interface (DVTI) configuration on a Cisco ASR 1000 Series Router may result in some tunnels not coming up.

  Workaround: Manually remove the failed tunnels, and reconnect each tunnel one at a time.

- CSCso86721

  On a Cisco ASR 1000 Series Router if a hierarchical policy-map is configured on a parent shaper, and a priority class with percent police is configured on a child policy that is attached to a subinterface, changing the parent shape rate while the policy is attached to the interface does not translate to a change in the police cir on the child.

  Workaround: Remove the policy from the interface and reattach it.

- CSCso92930

  With Authentication, Authorization, and Accounting (AAA) accounting enabled on a Cisco ASR 1000 Series Router, the available memory Route Processor (RP) decreases over time as subscribers connect and disconnect.

  This condition is observed when the Cisco ASR 1000 Series Router is functioning as an L2TP Access Concentrator (LAC) or L2TP Network Server (LNS), and AAA accounting is enabled for tunnel, session, and Point-to-Point Protocol (PPP).

  Workaround: If the available memory decrease impacts system functions, you may disable AAA accounting.

- CSCso97208

  On a Cisco ASR 1000 Series Router, repeatedly issuing **shut** and **no shut** commands on multilink bundles with multiple member links and a Quality of Service (QoS) service policy attached may trigger an unexpected reload of the Embedded Services Processor (ESP).

  Workaround: To avoid this condition, pause 5 seconds or more between the **shut** and **no shut** operations for individual multilink bundles with a QoS service-policy attached.

- CSCso97651

  On a Cisco ASR 1000 Series Router, running stateful traffic over dynamic IPSec tunnels for an extended period may lead to an unexpected reload of the Embedded Services Processor (ESP).

  Workaround: Use static IPSec tunnels instead of dynamic tunnels, if applicable.

- CSCso98733

  On a Cisco ASR 1000 Series Router, removing a Gateway Load Balancing Protocol (GLBP) configuration may cause a failure upon the Route Processor (RP) switchover, causing an outage of the router and a subsequent reload of both RPs.

  Workaround: Avoid removing a GLBP configuration after it is configured.

- CSCso98929

  Error trace messages are generated when Network Based Application Recognition (NBAR) traffic is run during a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

  Further Problem Description: The error trace is informational only and has no functional impact.

- CSCso99244

  On a Cisco ASR 1000 Series Router, an IOSd reset occurs when an attempt is made to attach an already configured Quality of Service (QoS) service policy to a zone-pair.

  Workaround: Ensure that any service policies that are to be attached to a zone-pair are all created as inspect service policies using the **policy-map type inspect** command.

- CSCso99480

  On a Cisco ASR 1000 Series Router with Route Processor (RP)/Embedded Services Processor (ESP) redundancy, the standby ESP may reload while building 2K Dynamic Virtual Tunnel Interface (DVTI) IPSec tunnels.

  Workaround: Use a dynamic crypto map instead of DVTI.

- CSCsq01759

  When an IPSec tunnel is configured between a Cisco ASR 1000 Series Router and a remote peer using tunnel interfaces through a network address translation (NAT) device, the router drops User Datagram Protocol (UDP) encapsulated encrypted packets

  This condition affects the following features:

  - IPSec/GRE with NAT
  - DMVP with NAT
  - VTI with NAT

  Workaround: Do not configure IPSec on tunnel interfaces.

- CSCsq03423

  On a Cisco ASR 1006 Router with two Cisco ASR1000-ESP10 boards, if the **clear ip tcp header-compression** or **clear ip rtp header-compression** command is executed after a Cisco ASR1000-ESP10 switchover, the new standby Cisco ASR1000-ESP10 may reset. The newly active Cisco ASR1000-ESP10 functions correctly after the switchover.

  There are no known workarounds.

- CSCsq03572

  On a Cisco ASR 1000 Series Router, an attempt to copy a Quality of Service (QoS) policy configuration to the running configuration using the Trivial File Transfer Protocol (TFTP) does not download the policy properly when traffic to the serial interfaces is enabled for FRF12.

  Workaround: Apply the QoS policy configuration without traffic over the interfaces.

Open Caveats—Cisco IOS XE Release 2.1.0

This section documents possible unexpected behavior by Cisco IOS XE Release 2.1.0.

- CSCsl49274

  A Cisco ASR 1000 Series Router may reset when the **show interface random-detect** command is executed.

  This condition occurs only when a policy map is configured with Weighted Random Early Detection (WRED) in the class-default class, and the policy map is applied to an interface.

  Workaround: Use the **show policy-map interface** command instead of the **show interface random-detect** command.

  Further Problem Description: The **show interface random-detect** command is a legacy QoS command and is not supported on the Cisco ASR 1000 Series Router.

- CSCsm05024

  After running traffic for an extended period of time on a Cisco ASR 1000 Series Router, a Route Processor (RP) switchover may result in a reload of the new standby RP when the RP attempts to synchronize the configuration.

  After an auto-reload, the standby RP again functions as expected.

  There are no known workarounds.

- CSCsm05560

  Default wred thresholds are calculated when wred instance is created. Once wred instance is configured with default thresholds, change in class bandwidth/queue-limit does not re-calculate default threshold values unless wred instance is removed and re-installed

  Workaround: Is to remove and re-install WRED feature.

- CSCsm49243

  On a Cisco ASR 1000 Series Router, **ip dhcp relay** commands (**ip dhcp relay information option server-id-override** and **ip dhcp relay source-interface Loopback0**) configured under interface range may not synchronize over to the newly active Route Processor (RP) after switchover.

  Workaround: Instead of using range commands, configure the interfaces individually.

- CSCsm55507

  On a Cisco ASR 1000 Series Router, when the IP MTU on a Generic Routing Encapsulation (GRE) tunnel interface exceeds that on the physical interface carrying tunnel traffic, the traffic requiring fragmentation may be dropped over time.

  Workaround: Configure an IP MTU on the tunnel interface no greater than that on the physical interface carrying tunnel traffic.

- CSCsm74141

  On a Cisco ASR 1000 Series Router, successive copying of qos configuration including issuing the **match access-group** command to the running configuration leads to duplicate entries for the match access-group clause.

  Workaround: This issue is strictly a **show configuration** issue and has no functional impact.

- CSCsm98756

  CPU usage peaks at 99 percent for a sustained period when the **show run | inc ipv6 route** command is issued with a large-scale configuration (thousands of VLANs) on a Cisco ASR 1000 Series Router, and various control plane functions such as Session Border Controller (SBC) call setup may not function as expected.

  Workaround: Reduce the **show run** command output to a file for post-processing.

- CSCso16581

  The TIE on line interfaces that use network clocking, such as OC3 and OC12, can oscillate and fail to meet the 100 second settling time requirement.

  This condition can occur when the network clock input (the source of timing distribution for the box) undergoes rapid changes in frequency offset. Note that this is a rare and unusual condition but still permissible. A 10 PPM delta (+5 to -5 PPM) across 10 seconds can result in a failure to meet the TIE in this case.

  Workaround: The problem can be mitigated by ensuring that there is no rapid frequency offset change on the reference clock. There is no full workaround.

- CSCso38119

  On a Cisco ASR 1000 Series Router, when control plane changes are made to Quality of Service (QoS), or subinterfaces are added that have a service policy applied when the physical interface associated with the control plane changes is over-subscribed, the following error message is reported on the console:

  ```
  CPPBQS-3-QMOVEFAIL: F0: cpp_cp: CPP 0 schedule InterfaceSchedule queue move failed
  (0xa6090402) - SEID=0x141 SID=0X280C1
  ```

  This severe condition will prohibit further configuration changes and cause inconsistencies between the control plane and data plane.

  Workaround: Avoid making control plane changes involving QoS when the physical interface associated with the changes is over-subscribed.

- CSCso61824

  Under rare conditions, a SPA fails to come online when the Cisco ASR 1000 Series Router is reloaded when the Route Processor (RP) is busy processing a large configuration. The SPA process experiences multiple resets.

  Workaround: To recover from the SPA failure condition, reload the SIP.

- CSCso71857

  A Packet-over-SONET (POS) SPA on the Cisco ASR 1000 Series Router incorrectly reports a line alarm indication signal (LAIS) alarm as a Section Bit Interleaved Parity alarm and issues the following error message:

  ```
  *Apr 9 11:09:47: %ASR1000_RP_SONET_ALARM-6-POS: ASSERT CRITICAL POS0/2/1 Section Bit
  Interleaved Parity
  ```

  There are no known workarounds.

- CSCso73923

  On a Cisco ASR 1000 Series Router, an unexpected reload of the Embedded Services Processor (ESP) may be seen if fair-queue is added to or deleted from an existing policy-map.

  This reload has been observed when a hierarchical Quality of Service (QoS) policy was modified to apply the **fair-queue** command as part of the existing child policy.

  Workaround: Detach the service-policy prior to modification, then re-attach the service-policy back to the interface.

- CSCso77028

  On Packet-over-SONET (POS) interfaces on a Cisco ASR 1000 Series Router with Network Based Application Recognition (NBAR) configured (Protocol discovery and/or service policies), changing the NBAR configuration, then repetitively adding and/or removing NetFlow may cause the Embedded Services Processor (ESP) to reload. The reload may occur during or after the point at which NetFlow is enabled or disabled.

  Workaround: When NBAR and NetFlow are configured on a POS interface, allow a delay of 30 seconds or more between removing the NBAR configuration and the configuration/de-configuration of NetFlow.

- CSCso81177

  On a Cisco ASR 1000 Series Router, if Network Address Translation (NAT) is configured immediately after Network Based Application Recognition (NBAR) is de-configured, an unpredictable internal state can result.

  Workaround: Configure NAT before de-configuring NBAR, or wait until all NBAR links are removed or expired.

- CSCso83252

  Connecting multiple IPSec tunnels at the same time or in quick succession using a Dynamic Virtual Tunnel Interface (DVTI) configuration on a Cisco ASR 1000 Series Router may result in some tunnels not coming up.

  Workaround: Manually remove the failed tunnels, and reconnect each tunnel one at a time.

- CSCso86721

  On a Cisco ASR 1000 Series Router if a hierarchical policy-map is configured on a parent shaper, and a priority class with percent police is configured on a child policy that is attached to a subinterface, changing the parent shape rate while the policy is attached to the interface does not translate to a change in the police cir on the child.

  Workaround: Remove the policy from the interface and reattach it.

- CSCso92930

  With Authentication, Authorization, and Accounting (AAA) accounting enabled on a Cisco ASR 1000 Series Router, the available memory Route Processor (RP) decreases over time as subscribers connect and disconnect.

  This condition is observed when the Cisco ASR 1000 Series Router is functioning as an L2TP Access Concentrator (LAC) or L2TP Network Server (LNS), and AAA accounting is enabled for tunnel, session, and Point-to-Point Protocol (PPP).

  Workaround: If the available memory decrease impacts system functions, you may disable AAA accounting.

- CSCso97208

  On a Cisco ASR 1000 Series Router, repeatedly issuing **shut** and **no shut** commands on multilink bundles with multiple member links and a Quality of Service (QoS) service policy attached may trigger an unexpected reload of the Embedded Services Processor (ESP).

  Workaround: To avoid this condition, pause 5 seconds or more between the **shut** and **no shut** operations for individual multilink bundles with a QoS service-policy attached.

- CSCso97651

  On a Cisco ASR 1000 Series Router, running stateful traffic over dynamic IPSec tunnels for an extended period may lead to an unexpected reload of the Embedded Services Processor (ESP).

  Workaround: Use static IPSec tunnels instead of dynamic tunnels, if applicable.

- CSCso98733

  On a Cisco ASR 1000 Series Router, removing a Gateway Load Balancing Protocol (GLBP) configuration may cause a failure upon the Route Processor (RP) switchover, causing an outage of the router and a subsequent reload of both RPs.

  Workaround: Avoid removing a GLBP configuration after it is configured.

- CSCso98929

  Error trace messages are generated when Network Based Application Recognition (NBAR) traffic is run during a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

  Further Problem Description: The error trace is informational only and has no functional impact.

- CSCso99244

  On a Cisco ASR 1000 Series Router, an IOSd reset occurs when an attempt is made to attach an already configured Quality of Service (QoS) service policy to a zone-pair.

  Workaround: Ensure that any service policies that are to be attached to a zone-pair are all created as inspect service policies using the **policy-map type inspect** command.

- CSCso99480

  On a Cisco ASR 1000 Series Router with Route Processor (RP)/Embedded Services Processor (ESP) redundancy, the standby ESP may reload while building 2K Dynamic Virtual Tunnel Interface (DVTI) IPSec tunnels.

  Workaround: Use a dynamic crypto map instead of DVTI.

- CSCsq01759

  When an IPSec tunnel is configured between a Cisco ASR 1000 Series Router and a remote peer using tunnel interfaces through a network address translation (NAT) device, the router drops User Datagram Protocol (UDP) encapsulated encrypted packets

  This condition affects the following features:

  - IPSec/GRE with NAT
  - DMVP with NAT
  - VTI with NAT

  Workaround: Do not configure IPSec on tunnel interfaces.

- CSCsq03423

  On a Cisco ASR 1006 Router with two Cisco ASR1000-ESP10 boards, if the **clear ip tcp header-compression** or **clear ip rtp header-compression** command is executed after a Cisco ASR1000-ESP10 switchover, the new standby Cisco ASR1000-ESP10 may reset. The newly active Cisco ASR1000-ESP10 functions correctly after the switchover.

  There are no known workarounds.

- CSCsq03572

  On a Cisco ASR 1000 Series Router, an attempt to copy a Quality of Service (QoS) policy configuration to the running configuration using the Trivial File Transfer Protocol (TFTP) does not download the policy properly when traffic to the serial interfaces is enabled for FRF12.

  Workaround: Apply the QoS policy configuration without traffic over the interfaces.