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:

- Introduction, page 2
- System Requirements, page 3
- New and Changed Information, page 33
- MIBs, page 138
- Limitations and Restrictions, page 141
- Important Notes, page 146
- Caveats, page 158

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

- Related Documentation, page 158
- Open Source License Notices, page 163
- Obtaining Documentation and Submitting a Service Request, page 165

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, page 3
- Cisco IOS XE Software Package Compatibility for ISSU, page 6
- Cisco IOS XE Release Compatibility Tables, page 7
- RP Memory Recommendations, page 19
- Hardware Supported, page 25
- ROMmon Version Requirements, page 25
- Determining the Software Version, page 27
- Upgrading to a New Software Release, page 33
- Cisco IOS XE to Cisco IOS Version Number Mapping, page 32

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, page 34
- New Software Features in Cisco IOS XE Release 2.6.2, page 34
- New Hardware Features in Cisco IOS XE Release 2.6.1, page 35
- New Software Features in Cisco IOS XE Release 2.6.1, page 35
- New Hardware Features in Cisco IOS XE Release 2.6.0, page 37
- New Software Features in Cisco IOS XE Release 2.6.0, page 38
- New Hardware Features in Cisco IOS XE Release 2.5.2, page 50
- New Software Features in Cisco IOS XE Release 2.5.2, page 50
- New Hardware Features in Cisco IOS XE Release 2.5.1, page 50
- New Software Features in Cisco IOS XE Release 2.5.1, page 50
- New Hardware Features in Cisco IOS XE Release 2.5.0, page 51
- New Software Features in Cisco IOS XE Release 2.5.0, page 52
- New Hardware Features in Cisco IOS XE Release 2.4.3, page 69
- New Software Features in Cisco IOS XE Release 2.4.3, page 69
- New Hardware Features in Cisco IOS XE Release 2.4.4, page 69
- New Software Features in Cisco IOS XE Release 2.4.4, page 69
- New Hardware Features in Cisco IOS XE Release 2.4.2t, page 69
- New Software Features in Cisco IOS XE Release 2.4.2t, page 69
- New Hardware Features in Cisco IOS XE Release 2.4.2, page 70
- New Software Features in Cisco IOS XE Release 2.4.2, page 70

- New Software Features in Cisco IOS XE Release 2.4.1, page 70
- New Hardware Features in Cisco IOS XE Release 2.4.0, page 72
- New Software Features in Cisco IOS XE Release 2.4.0, page 73
- New Hardware Features in Cisco IOS XE Release 2.3.2, page 93
- New Software Features in Cisco IOS XE Release 2.3.2, page 93
- New Hardware Features in Cisco IOS XE Release 2.3.1, page 93
- New Software Features in Cisco IOS XE Release 2.3.1, page 93
- New Hardware Features in Cisco IOS XE Release 2.3.0, page 93
- New Software Features in Cisco IOS XE Release 2.3.0, page 94
- New Hardware Features in Cisco IOS XE Release 2.2.3, page 106
- New Software Features in Cisco IOS XE Release 2.2.3, page 106
- New Hardware Features in Cisco IOS XE Release 2.2.2, page 107
- New Software Features in Cisco IOS XE Release 2.2.2, page 107
- New Hardware Features in Cisco IOS XE Release 2.2.1, page 107
- New Software Features in Cisco IOS XE Release 2.2.1, page 109
- New Hardware Features in Cisco IOS XE Release 2.1.2, page 124
- New Software Features in Cisco IOS XE Release 2.1.2, page 124
- New Hardware Features in Cisco IOS XE Release 2.1.1, page 124
- New Software Features in Cisco IOS XE Release 2.1.1, page 124
- New Hardware Features in Cisco IOS XE Release 2.1.0, page 125
- New Software Features in Cisco IOS XE Release 2.1.0, page 130
- Release Note Only Software Features in Cisco IOS XE Release 2.1.0, page 134

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, page 35
- CUBE(SP Edition) - Billing:Packet Cable Billing support for Adjacency Information, page 35
- OER - Application Aware Routing with Static Application Mapping, page 35
- OER Border Router Only Functionality, page 36
- OER - Inbound Optimization through BGP, page 36
- OER Port and Protocol Based Prefix Learning, page 36
- OER Support for Cost-Based Optimization and Traceroute Reporting, page 36
- OER Support for Policy-Rules Configuration and Port-Based Prefix Learning, page 36
- OER VPN IPSec with GRE Tunnel Optimization, page 36
- OER - Voice Traffic Optimization, page 37
- PfR EIGRP mGRE DMVPN Hub-and-Spoke Support, page 37
- PfR - Protocol Independent Route Optimization (PIRO), page 37

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, page 39
- ASRNAT - Overload Scaling Improvement - Support 800 Overloaded Pools, page 39
- BGP Event Based VPN Import, page 39
- BGP RT Changes Without PE-CE Neighbor Impact, page 40
- BGP Support for the L2VPN Address Family, page 40
- Broadband IPv6 Support at LNS, page 40
- Call Home, page 40
- CLNS Support for GRE Tunneling of IPv4 and IPv6, page 40
- Control Plane DSCP Support for RSVP, page 40
- DHCP VRF Exclude Support, page 41
- EIGRP Prefix Limit Support, page 41
- Enabling OSPFv2 on an Interface Basis, page 41
- IGMP MIB Support Enhancements for SNMP, page 41
- IGMP Static Group Range Support, page 41
- IGMPv3 Host Stack, page 41
- IP-RIP Delay Start, page 42
- IPv6 - Full Selective Packet Discard (SPD) Support, page 42
- IPv6 - Per Interface Neighbor Discovery Cache Limit, page 42
- IPv6 ISIS Local RIB, page 42
- IPv6 Multicast: Bandwidth-Based Call Admission Control (CAC), page 42
- IPv6 PIM Passive, page 42
- IPv6 Routing: IS-IS Multitopology Support for IPv6, page 42
- IPv6: Multicast Address Group Range Support, page 43
- IS-IS Fast-Flooding of LSPs Using the fast-flood Command, page 43
- IS-IS Limit on Number of Redistributed Routes, page 43
- IS-IS Support for Route Tags, page 43
- Lawful Intercept (LI), page 43
- Layer 2 Tunnel Protocol Version 3, page 44
- MLD Group Limits, page 44
- MPLS MTU command for GRE Tunnels, page 44
- MPLS TE--Tunnel-Based Admission Control (TBAC), page 44
- Multicast Address Group Range Support, page 45
- Multicast MIB VRF Support, page 45
- Multiprotocol BGP (MP-BGP) Support for CLNS, page 45

- http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_sup_clns_xe.html, page 45
- OSPF Link-State Advertisement Throttling, page 45
- OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements, page 46
- OSPF Sham-Link MIB Support, page 46
- OSPF SNMP ifIndex Value for Interface ID, page 46
- OSPF Limit on Number of Redistributed Routes, page 46
- PIM Triggered Joins, page 46
- Quality of Service: Policies Aggregation, page 46
- RSVP Aggregation, page 47
- RSVP Application ID Support, page 47
- RSVP Fast Local Repair (RSVP FLR), page 47
- RSVP Interface-based Receiver Proxy, page 47
- RSVP Scalability Enhancements, page 47
- RSVP Support for IP Sessions, page 47
- SNMP Traps for PPPoE Session Limits, page 47
- Support for Software Media Termination Point (MTP) on the Cisco Unified Border Element (Enterprise), page 48
- T.38 Fax Support on the Cisco Unified Border Element (Enterprise), page 48
- VRF Aware IPSec, page 48
- VRRP MIB - RFC2787, page 48
- VRRP: Virtual Router Redundancy (VRRS), page 49
- Zone Based Firewall: Default Zone, page 49
- Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model, page 49

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 limi**t <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), page 51
- New XFP/SFPs Supported with SPAs and the Built-In Gigabit Ethernet Interface, page 51

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, page 54
- AAA - Improvements for Broadband IPv6, page 54
- ANCP - ATM Support, page 54
- ATM F4 Ping, page 54
- ATM Sub-interface Multipoint, page 54
- BGP Best External, page 55
- BGP Multicast Inter-AS (IAS) VPN, page 55
- BGP VPLS Auto Discovery Support on Route Reflector, page 56
- Configurable Domain Name Prefix and Suffix Stripping, page 56
- DHCP - DHCPv6 Prefix Delegation RADIUS VSA, page 56
- DHCP Enhancements to Support IPv6 Broadband Deployments, page 56
- DHCPv6 Repackaging, page 56
- DMVPN Manageability Enhancements, page 56
- DMVPN: Dynamic tunnels between spokes behind NAT, page 57
- Dynamic Subscriber Bandwidth Selection, page 57
- EtherChannel Min-Links, page 57
- Firewall - VRF-aware ALG support, page 57
- Flow Based Per Port Channel Load Balancing, page 57
- IEEE 802.3ad - Faster Link Switchover Time, page 58
- IEEE 802.3ad MIB, page 58
- IPv6 Access Services: AAA Support for Cisco VSA IPv6 Attributes, page 58

- IPv6 Access Services: AAA Support for RFC 3162 IPv6 RADIUS Attributes, page 58
- IPv6 Access Services: PPPoA, page 58
- IPv6 Access Services: PPPoE, page 58
- IPv6 Access Services: Stateless DHCPv6, page 59
- ISG:AAA Wireless Enhancements, page 59
- ISG:Accounting: Prepaid, page 59
- ISG:Authentication:Radius Proxy WiMax Enhancements, page 59
- ISG:Instrumentation:DHCP Lease Query Support, page 59
- ISG:Policy Control:Differentiated Initial Policy Control, page 59
- ISG:Session: Creation: Interface IP Session: L2, page 60
- ISG:Session: Creation: Interface IP Session: L3, page 60
- ISG:Session:Multicast:Coexistance, page 60
- ISG:Session:Static Session Creation, page 60
- ISSU - Multicast MPLS VPN, page 60
- ISSU – PPPoEoA, page 60
- Layer 2 Local Switching - Same-Port Switching for Ethernet VLAN, page 61
- Layer 2 Local Switching: Ethernet to VLAN, page 61
- Link Aggregation Control Protocol (LACP) (802.3ad) for Gigabit Interfaces, page 61
- Local Template-Based ATM PVC Provisioning, page 61
- MPLS VPN Half Duplex VRF (HDVRF), page 61
- MSDP MD5 password authentication, page 62
- Multicast VPN Extranet Support, page 62
- Multicast VPN Extranet VRF Select, page 62
- Multicast VPN Inter-AS Support, page 62
- Multicast VPN MIB, page 62
- Multicast-VPN: Multicast Support for MPLS VPN, page 63
- NAT - VRF aware NAT for MPLS/VPN, page 63
- NAT - VRF-aware ALG support, page 63
- NBAR PDLM supported in ASR1000 Release 5, page 63
- NHRP - CEF rewrite for DMVPN Phase 3 Networks, page 63
- NHRP MIB for DMVPN Networks, page 64
- NSF/SSO - Multicast MPLS VPN, page 64
- PPP Enhancement for Broadband IPv6, page 64
- PPP Session Queueing on ATM VC, page 64
- PPPoE Connection Throttling, page 64
- PPPoE on ATM, page 64
- PPPoE Session Count MIB, page 65
- QoS: QoS support for GRE/sVTI Tunnel, page 65

- QoS: Shape Average Percent CLI, page 65
- Service Advertisement Framework (SAF), page 65
- SSO - LACP, page 65
- SSO - PPPoE IPv6, page 66
- SSO - PPPoEoA, page 66
- VRF Aware Cisco IOS Firewall, page 66
- Cisco Unified Border Element (Enterprise), page 66
- Cisco Unified Border Element (SP Edition), page 67

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, page 141
- Limitations and Restrictions in Cisco IOS XE Release 2.2.3, page 142
- Limitations and Restrictions in Cisco IOS XE Release 2.2.1, page 143
- Limitations and Restrictions in Cisco IOS XE Release 2.1.1, page 144
- Limitations and Restrictions in Cisco IOS XE Release 2.1.0, page 145

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/fsacl

seq.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, page 159
- Cisco Feature Navigator, page 162
- Error Message Documentation for Cisco IOS XE Release 2, page 162
- Cisco IOS XE Software Documentation Set, page 162

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 Guid*e

  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

Original SSLeay License:

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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.