Cisco CSR 1000V Series Cloud Services Router Release Notes

First Published: April 1, 2013
Last Updated: February 3, 2014
OL-26569-09

This release notes document provides information about Cisco CSR 1000V Series Cloud Services Routers Release 3S up to and including Cisco IOS XE 3.11S.

Cisco CSR 1000V Series Cloud Services Routers Overview

The Cisco CSR 1000V Cloud Services Router provides a cloud-based virtual router that is deployed on a virtual machine (VM) instance on x86 server hardware. The Cisco CSR 1000V router is a virtual platform that provides selected Cisco IOS XE security and switching features on a virtualization platform.

When the Cisco CSR 1000V virtual IOS XE software is deployed on a VM, the Cisco IOS software functions just as if it were deployed on a traditional Cisco hardware platform. You can configure different features depending on the supported Cisco IOS XE software image. The Cisco CSR 1000V supports a subset of Cisco IOS XE software features and technologies.

The Cisco CSR 1000V provides secure connectivity from the enterprise premise (such as a branch office or data center) to the public or private cloud.

Cisco IOS XE 3S Releases and Cisco IOS Release Number Mapping

The Cisco CSR 1000 Series Cloud Services Routers releases correspond to the Cisco IOS XE releases. For example, Cisco IOS XE Release 3.11(0) is the software release for Cisco CSR 1000V Series Cloud Services Routers Release 3.11(0).

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

Table 1 Cisco IOS XE 3S–to–Cisco IOS Release Number Mapping

Cisco IOS XE 3S Release	Cisco IOS Release
3.9(0)	15.3(2)S
3.10(0)	15.3(3)S
3.11(0)	15.4(1)S

Feature Navigator

You can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on cisco.com is not required.

System Requirements

The following sections describe the system requirements for the Cisco CSR 1000V Series Cloud Services Routers.

- Hardware Requirements
- Software Images and Licenses

Hardware Requirements

- Hardware Requirements (Cisco IOS XE 3.10S and Later)
- Hardware Requirements (Cisco IOS XE 3.8S and 3.9S)

Hardware Requirements (Cisco IOS XE 3.10S and Later)

For installation and hardware requirements, see the *Cisco CSR 1000V Series Cloud Services Router Software Configuration Guide*.

Hardware Requirements (Cisco IOS XE 3.8S and 3.9S)

The Cisco CSR 1000V router is a virtual machine, and can be supported on selected x86 hardware.

The following are the minimum requirements for the Cisco IOS XE 3.8S and 3.9S releases.

- The Cisco CSR 1000V router VM:
  - 4 virtual CPUs
  - 4 GB RAM
  - 8 GB Hard Drive
- PC running the VMware vSphere Client 5.0
- Server running VMware ESXi 5.0
  - CPU: Intel Nehalem or later is required.
  - Hardware Compatibility: Must be listed as supported on the VMware Hardware Compatibility List.

    The Cisco CSR 1000V is supported on all Cisco UCS servers. Table 2 lists the Cisco UCS and non-Cisco servers that have been tested for compatibility.

Table 2 Servers Tested with Cisco CSR 1000V Release 3.9(0)S

Vendor	Servers Tested for Compatibility
Cisco	• UCS B230 M2 • UCS C220 M3 • UCS C210 M2 • UCS C200 M2 • UCS B22 M3
HP	• HP ProLiant DL180G6
Dell	• Dell R720 with Xeon® E5-2660

Note Cisco UCS B230-M2, B440-M2, C260-M2, and C460-M2 servers with Intel Westmere-EX CPUs require UCS release 2.0(4) or later.

  - Memory: 16GB DDR3 or higher
  - Hard Drive: 100GB or higher
  - Network Cards: 1 Gbps (3 or higher)
  - The minimum clock rate supported is 1.9 Ghz

Note The Cisco CSR 1000V router supports a maximum of 10 vNICs (the maximum supported by ESXi 5.0)

Software Images and Licenses

Cisco CSR 1000V Software Licenses for Cisco IOS XE 3.10Sand 3.11S

Cisco CSR 1000V software licenses are divided into the following feature set technology packages:

- Standard Package: Basic Networking Routing (Routing, HSRP, NAT, ACL, VRF, GRE)
- Advanced Package: Standard package + Security (IP Security VPN, Firewall, MPLS, Multicast, QoS)
- Premium Package: Standard + Advanced Networking (AppNav, AVC, OTV and LISP)

For more information about the Cisco IOS XE technologies supported in the feature set packages, see the overview chapter of the *Cisco CSR 1000V Cloud Services Router Software Configuration Guide.*

The Cisco CSR 1000V router provides both perpetual licenses and term subscription licenses that support the feature set packages for the following maximum throughput levels:

- 10 Mbps
- 50 Mbps
- 100 Mbps
- 250 Mbps
- 500 Mbps
- 1 Gbps

Not all maximum throughput levels are available for all feature set technology packages. For more information about how the maximum throughput levels are regulated on the router, see the installation chapter of the *Cisco CSR 1000V Cloud Services Router Software Configuration Guide.*

Beginning with Cisco IOS XE 3.10S, a memory upgrade license is available to add memory to the Cisco CSR 1000V. This license is available only for selected technology packages.

In addition, the Cisco CSR 1000V offers a 60-day evaluation license. The evaluation license is for the Premium technology package, although you can use the **license boot-level** command to change to either the Standard or Advanced package level. The evaluation license is limited to 10, 25 or 50 Mbps throughput.

Table 3 lists the Cisco CSR 1000V licenses for Cisco IOS XE 3.10S and 3.11S.

- Note that the maximum throughput levels are based on performance using VMware ESXi. The maximum throughput if using either Citrix XenServer or a KVM-based hypervisor may be lower.
- The server resource requirements for virtual CPU configuration and RAM allocation depend on the throughput license and technology package installed. For more information, see the Cisco CSR 1000V data sheet for your release.

Note License SKUs shown in **bold** are available only through a service representative.

Table 3 Cisco CSR 1000V License SKUs for Cisco IOS XE 3.10S and 3.11S

License SKU	Description	Maximum number of IPsec tunnels supported
Subscription Term Licenses:		
L-CSR-100M-ADV-1Y= L-CSR-100M-ADV-3Y=	1-year and 3-year licenses for 100 Mbps maximum for the Advanced package.	400
L-CSR-100M-PRM-1Y= L-CSR-100M-PRM-3Y=	1-year and 3-year licenses for 100 Mbps maximum for the Premium package.	400
L-CSR-250M-ADV-1Y= **L-CSR-250M-ADV-3Y=**	1-year and 3-year licenses for 250 Mbps maximum for the Advanced package.	400
L-CSR-250M-PRM-1Y= **L-CSR-250M-PRM-3Y=**	1-year and 3-year licenses for 250 Mbps maximum for the Premium package.	400
L-CSR-500M-STD-1Y= L-CSR-500M-STD-3Y=	1-year and 3-year licenses for 500 Mbps maximum for the Standard package.	400
L-CSR-1G-STD-1Y= L-CSR-1G-STD-3Y=	1-year and 3-year licenses for 1 Gbps maximum for the Standard package.	400
Perpetual Licenses:		
L-CSR-10M-STD= L-CSR-10M-ADV= L-CSR-10M-PRM=	Perpetual licenses for 10 Mbps maximum for Standard, Advanced and Premium packages.	150
L-CSR-50M-STD= L-CSR-50M-ADV= L-CSR-50M-PRM=	Perpetual licenses for 50 Mbps maximum for Standard, Advanced and Premium packages.	150
L-CSR-100M-STD= L-CSR-100M-ADV= L-CSR-100M-PRM=	Perpetual licenses for 100 Mbps maximum for Standard, Advanced and Premium packages.	150 for the Standard package 400 for the Advanced and Premium packages
L-CSR-250M-STD= **L-CSR-250M-ADV=** **L-CSR-250M-PRM=**	Perpetual licenses for 250 Mbps maximum for Standard, Advanced and Premium packages.	150 for the Standard package 400 for the Advanced and Premium packages
L-CSR-500M-STD=	Perpetual licenses for 500 Mbps maximum for Standard package.	400
L-CSR-1G-STD=	Perpetual license for 1 Gbps maximum for the Standard package.	400

Table 3 Cisco CSR 1000V License SKUs for Cisco IOS XE 3.10S and 3.11S (continued)

License SKU	Description	Maximum number of IPsec tunnels supported
Memory Upgrade License (Cisco IOS XE 3.11S only):		
L-CSR-500M-PRM-8G=	Memory upgrade license to add up to 8 GB memory with route reflector support for the 500 Mbps maximum Premium package. **Note** The additional memory is allocated to IOSD memory on the Cisco CSR 1000V and is not used for adding memory on the VM.	400

For more information about each software license, including part numbers, see the Cisco CSR 1000V Router Datasheet. For more information about the standard Cisco IOS XE software activation procedure, see the *Software Activation Configuration Guide, Cisco IOS XE Release 3S*.

Cisco CSR 1000V Software Licenses for Cisco IOS XE 3.9

Cisco CSR 1000V software licenses are divided into the following feature set technology packages:

- Standard Package: Basic Networking Routing (Routing, HSRP, NAT, and VLAN)
- Advanced Package: Standard package + Security (Firewall, and VPN)
- Premium Package: Standard + Advanced Networking (AppNav, MPLS, QoS, AVC, and LISP)

The Cisco CSR 1000V router provides term subscription licenses that support the feature set packages for the following maximum throughput levels:

- 10 Mbps
- 25 Mbps
- 50 Mbps

Table 4 lists the Cisco CSR 1000V licenses for Cisco IOS XE 3.9S. All licenses support a maximum of 150 IPsec tunnels.

Table 4 Cisco CSR 1000V License SKUs for Cisco IOS XE 3.9S

License SKU	Description
L-CSR-10M-STD-1Y=	1-Year License for 10 Mbps maximum Standard Package
L-CSR-10M-STD-3Y=	3-Year License for 10 Mbps maximum Standard Package
L-CSR-10M-STD-5Y=	5-Year License for 10 Mbps maximum Standard Package
L-CSR-10M-ADV-1Y=	1-Year License for 10 Mbps maximum Advanced Package
L-CSR-10M-ADV-3Y=	3-Year License for 10 Mbps maximum Advanced Package
L-CSR-10M-ADV-5Y=	5-Year License for 10 Mbps maximum Advanced Package
L-CSR-10M-PRM-1Y=	1-Year License for 10 Mbps maximum Premium Package

Table 4 Cisco CSR 1000V License SKUs for Cisco IOS XE 3.9S (continued)

License SKU	Description
L-CSR-10M-PRM-3Y=	3-Year License for 10 Mbps maximum Premium Package
L-CSR-10M-PRM-5Y=	5-Year License for 10 Mbps maximum Premium Package
L-CSR-25M-STD-1Y=	1-Year License for 25 Mbps maximum Standard Package
L-CSR-25M-STD-3Y=	3-Year License for 25 Mbps maximum Standard Package
L-CSR-25M-STD-5Y=	5-Year License for 25 Mbps maximum Standard Package
L-CSR-25M-ADV-1Y=	1-Year License for 25 Mbps maximum Advanced Package
L-CSR-25M-ADV-3Y=	3-Year License for 25 Mbps maximum Advanced Package
L-CSR-25M-ADV-5Y=	5-Year License for 25 Mbps maximum Advanced Package
L-CSR-25M-PRM-1Y=	1-Year License for 25 Mbps maximum Premium Package
L-CSR-25M-PRM-3Y=	3-Year License for 25 Mbps maximum Premium Package
L-CSR-25M-PRM-5Y=	5-Year License for 25 Mbps maximum Premium Package
L-CSR-50M-STD-1Y=	1-Year License for 50 Mbps maximum Standard Package
L-CSR-50M-STD-3Y=	3-Year License for 50 Mbps maximum Standard Package
L-CSR-50M-STD-5Y=	5-Year License for 50 Mbps maximum Standard Package
L-CSR-50M-ADV-1Y=	1-Year License for 50 Mbps maximum Advanced Package
L-CSR-50M-ADV-3Y=	3-Year License for 50 Mbps maximum Advanced Package
L-CSR-50M-ADV-5Y=	5-Year License for 50 Mbps maximum Advanced Package
L-CSR-50M-PRM-1Y=	1-Year License for 50 Mbps maximum Premium Package
L-CSR-50M-PRM-3Y=	3-Year License for 50 Mbps maximum Premium Package
L-CSR-50M-PRM-5Y=	5-Year License for 50 Mbps maximum Premium Package

For more information about each software license, including part numbers, see the Cisco CSR 1000V Router Datasheet. For more information about the standard Cisco IOS XE software activation procedure, see the *Software Activation Configuration Guide, Cisco IOS XE Release 3S*.

Cisco CSR 1000V Software Licenses for Cisco IOS XE 3.8S

- The Cisco CSR 1000V router offers the following subscription licenses for Cisco IOS XE Release 3.8S (Controlled Availability release):
- One year (L-CSR-ELS-50M-1Y=)
- Three year (L-CSR-ELS-50M-3Y=)
- Five year (L-CSR-ELS-50M-5Y=)

The licenses support a maximum throughput of 50 Mbps. In addition, the Cisco CSR 1000V offers a 60-day evaluation license.

For more information about the standard Cisco IOS XE software activation procedure, see the *Software Activation Configuration Guide, Cisco IOS XE Release 3S*.

Software Image Nomenclature for OVA Installation File

The Cisco CSR 1000V OVA installation file nomenclature indicates properties supported by the router in a given release.

The following is an example of an .ova installation filename for Cisco IOS XE 3.9S:

csr1000v-adventerprisek9.03.09.00a.S.153-2.S0a-C4-M4G-N3-D8.ova

Table 5 lists the attributes and the release properties indicated.

Table 5 OVA Installation Filename Attributes

Filename Attribute	Properties
adventerprisek9	Indicates the installed image package for the Cisco CSR 000V. In this case, the filename is for the Cisco IOS XE Advanced Enterprise package.
03.09.00a.S.153-2.S0a	Indicates that the software image is for the Cisco IOS XE 3.9.0aS release image (mapped to the Cisco IOS 15.3(2) release).
C4	Indicates that the software image supports 4 CPUs on the VM.
M4G	Indicates that the software image requires 4 GB memory on the VM.
N3	Indicates that the .ova image installs 3 vNICS. **Note** The Cisco CSR 1000V supports up to 10 vNICs in Cisco IOS XE 3.9S. The .ova installation process installs 3 vNICS. The remaining vNICS must be manually installed on the VM.
D8	Indicates that the software image requires an 8 GB hard disk.

Limitations and Restrictions in Cisco CSR 1000V Series Cloud Services Routers

Limitations and Restrictions in Cisco IOS XE 3.10S

This section lists limitations and restrictions on the Cisco CSR 1000V Series Cloud Services Router in Cisco IOS XE 3.10S.

- Configuring Network Based Application Recognition (NBAR), or Application Visibility and Control (AVC) support on the Cisco CSR 1000V requires a minimum of 4GB DRAM on the VM, even when using the 1 vCPU configuration on the VM.

- On the Cisco CSR 1000V, all the NICs are logically named as the Gigabit Ethernet interface. The Cisco CSR 1000V does support the 10G IXGBE vNIC in passthrough mode; but that interface also is also logically named as a Gigabit Ethernet interface. Note that with emulated devices like VMXNET3/PV/VIRTIO from the hypervisor, the Cisco CSR 1000V is not aware of the underlying interfaces. The vSwitch may be connected to a 10 GB physical NIC or 1 GB physical NICs or multiple NICs (with NIC teaming on the hypervisor) as well.
- The following limitations have been observed on the Cisco CSR 1000V with the 1 vCPU configuration with 2.5 GB of RAM allocation on VMware ESXi:
  - If the memory Hot-Add option is enabled, and the Cisco CSR 1000V is powered on with 2.5GB initial memory, then the RAM allocation can only increase to a maximum of 3 GB. The system does not allow upgrading to more than 3GB of RAM allocation. The Virtual Machine Properties windows shows “Maximum Hot-Add Memory for this Power is 3 GB”.
  - If the Cisco CSR 1000V is powered on with 3GB initial RAM allocation, then the Hot-Add memory option doesn't work, and the option to select memory remains greyed out with the same message on the Properties windows, “Maximum Hot-Add Memory for this Power is 3 GB”.
  - If the Cisco CSR 1000V is powered up with 4GB initial RAM allocation, then the Hot-Add options works and you are able to add up to 64 GB of memory.

Limitations and Restrictions in Cisco IOS XE 3.9S

This section lists limitations and restrictions on the Cisco CSR 1000V Series Cloud Services Router.

- You may experience low virtual network I/O performance with an Intel 1 Gbps NIC using the igb driver. Cisco recommends that you use a 10G NIC for higher throughput applications. For more information, see the VMware document at the following location and apply the settings:

  http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2018891
- The ESXi host power management policy should be set to High Performance. If this power management policy is not set, the Cisco CSR 1000V VM will crash due to the High Availability stuck thread detection not seeing the core running the data plane/ppe run for an extended period of time.

Limitations and Restrictions in Cisco IOS XE 3.8S

This section lists limitations and restrictions on the Cisco CSR 1000V Series Cloud Services Router.

- Four virtual CPUs are required per Cisco CSR 1000V router VM.
- In cases where there are multiple Cisco CSR 1000V routers, the total number of virtual CPUs and number of physical cores configured cannot exceed the number of physical cores - 1.
- Do not schedule on core zero.
- No VMs should span physical sockets.
- Frequency should be set to the frequency of the physical core.
- When the Cisco CSR 1000V first boots, the CSR feature license must be activated using the **license feature csr** command. The network interfaces on the router are disabled and cannot pass data traffic until the license is activated.
- ROMMON is not supported on the Cisco CSR 1000V router (applies to all releases).

New Features in and Important Notes about Cisco CSR 1000V Cloud Services Routers Release 3.11S

New Platform Features in Cisco IOS XE 3.11S

This section describes the new features supported on the Cisco CSR 1000V Series Cloud Services Router in Cisco IOS XE 3.11S that are specific to this platform. For more information about these features, see the *Cisco CSR 1000V Cloud Services Router Software Configuration Guide*.

Cisco CSR1000V 2vCPU Configuration

Beginning with Cisco IOS XE 3.11S, the Cisco CSR 1000V offers a configuration option that uses 2 virtual CPUs (vCPUs).

Memory Upgrade License

Beginning with this release, the Cisco CSR 1000V provides a memory upgrade license to add up to 8 GB memory with route reflector support for the 500 Mbps maximum Premium package. For more information, see the "Cisco CSR 1000V Software Licenses for Cisco IOS XE 3.10Sand 3.11S" section on page 4.

Deployment of the Cisco CSR 1000V on an Amazon Machine Image (AMI)

Beginning with this release, the Cisco CSR 1000V supports deployment on an Amazon Machine Image (AMI). You can deploy a Bring Your Own License (BYOL) AMI using a license purchased from Cisco. For more information, see the *Cisco CSR 1000V Series Cloud Services Router Deployment Guide for Amazon Web Services*.

VxLAN Layer 2 and Layer 3 Gateway Support on the Cisco CSR 1000V

This release provides VxLAN (Virtual eXtensible Local Area Network) Layer 2 and Layer 3 support on the Cisco CSR 1000V. VxLAN is a technology that provides a Layer-2 overlay network, allowing for network isolation. The standard 802.1q VLAN implementation limits the number of tags to 4,096. However, cloud service providers may want to operate more than 4,096 virtual networks. VxLAN uses a 24-bit network ID, which allows for a much larger number of individual identified networks to be operated.

For more information, see the *Cisco CSR 1000V VxLAN Support* document.

New and Modified REST API Support

Beginning in this release, the Cisco CSR 1000V REST API supports the following technologies:

- VRF
- EzVPN

The following REST APIs have been modified in this release:

- Global parameters
- ACL

For more information, see the *Cisco CSR 1000V Series Cloud Services Router REST API Management Reference Guide*.

Support for Remote Management by Cisco Prime Network Services Controller

The Cisco CSR 1000V supports remote management of the router using Cisco Prime Network Services Controller. For more information, see the *Cisco CSR 1000V Cloud Services Router Software Configuration Guide*. and the *Cisco Prime Network Services Controller* documentation.

New Cisco IOS XE Software Features in Cisco IOS XE 3.11S

This section describes new features in Cisco IOS XE 3.11S that are supported on the Cisco CSR 1000V Series Cloud Services Router and on other platforms.

New Cisco IOS XE Software Feature in Cisco IOS XE 3.11.0S

- Cisco Application Visibility and Control (AVC) Support in Cisco IOS XE 3.11S:

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios/solutions_docs/avc/ios_15.4_1T_ios_xe3_11/avc_user_guide_ios_15.4_1T_iosxe3_11.html

- Disjoint LISP RLOC Domains Support

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-lisp-support-for-disjoint-rloc-domains.html

- Enabling ALGs and AICs in Zone-Based Policy Firewalls

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/zbf-enable-alg-aic.html

- FNF: Prevent Export Storms

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/xe-3s/fnf-prevent-export-storms.html

- IOS IKEv2 support for AutoReconnect feature of AnyConnect

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-mt/sec-cfg-recon-flex.html

- IP Tunnel - GRE Key Entropy Support

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/configuration/xe-3s/ir-tunls-gre-entropy-xe.html

- IPV4 ACL Chaining Support

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-ip4-acl-chng-sup.html

- ISIS - Remote LFA FRR

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/15-2s/irs-rmte-lfa-frr.html

- LISP ESM Multihop Mobility

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-lisp-esm-multihop-mobility.html

- MPLS VPN over mGRE

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/configuration/xe-3s/ir-mpls-vpnomgre-xe.html

- NBAR2 Integrated Protocol Pack 6.0.0

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/pp600/nbar-prot-pack600.html

- OSPF LFA IPFRR Phase 3

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s//iro-ipfrr-lfa.html

- Per Tunnel QoS

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-3s/sec-conn-dmvpn-per-tunnel-qos.html

- TCP MSS Adjust

  For detailed information, see the following Cisco document:

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

New Features in and Important Notes about Cisco CSR 1000V Cloud Services Routers Release 3.10S

New Platform Features in Cisco IOS XE 3.10S

This section describes the new features supported on the Cisco CSR 1000V Series Cloud Services Router in Cisco IOS XE 3.10S that are specific to this platform. For more information about these features, see the *Cisco CSR 1000V Cloud Services Router Software Configuration Guide*.

New Higher Throughput-Based Licenses

Beginning in Cisco IOS XE 3.10S, Cisco CSR 1000V licenses based on higher maximum supported throughput levels are available. You can purchase licenses to support a maximum throughput level of 100 Mbps, 250 Mbps, 500 Mbps, or 1 Gbps. The maximum throughput licenses for 10 Mbps and 50 Mbps introduced in Cisco IOS XE 3.9S are still supported; the throughput licenses for 25 Mbps are no longer supported. For more information, see the "Cisco CSR 1000V Software Licenses for Cisco IOS XE 3.10Sand 3.11S" section on page 4 and the *Cisco CSR 1000V Cloud Services Router Software Configuration Guide*.

Cisco CSR1000V Low Footprint (1vCPU, 2.5Gb memory)

Beginning with Cisco IOS XE 3.10S, the Cisco CSR 1000V offers a low footprint configuration option that requires only 1 virtual CPU (vCPU) and 2.5 Gb memory. This option is only supported on VMware ESXi.

Support for Citrix XenServer Hypervisor

The Cisco CSR 1000V supports installation on the Citrix XenServer hypervisor, version 6.02.

Support for Kernel Virtual Module (KVM)-Based Hypervisors

The Cisco CSR 1000V supports installation on the following KVM-based hypervisors:

- KVM hypervisors based on Red Hat Enterprise Linux 6.3 and QEMU 0.12
- Red Hat Enterprise Virtualization 3.6

Additional VMware ESXi 5.0 Features Supported in Cisco IOS XE 3.10S

The following VMware ESXi 5.0 features are supported on the Cisco CSR 1000V Cloud Services Router beginning in Cisco IOS XE 3.10S:

- Distributed Resources Scheduler
- Fault Tolerance

Support for VMware ESXi 5.1

The Cisco CSR 1000V supports VMware ESXi 5.1 beginning with this release.

REST API Support for the Cisco CSR 1000V

Beginning with Cisco IOS XE 3.10S, the Cisco CSR 1000V provides support for RESTful APIs as an alternative to configuring the router using the Cisco IOS XE CLI. The REST API support is limited to the following technologies:

- Token-services
- Global
- Host-name, Domain-name, local-users, running-config, DNS servers, NTP
- Interface
- DHCP
- Routing (OSPF, BGP, EIGRP)
- ACL (IOS extended ACL)
- NAT
- ZBFW (Zone Based Firewall)
- IPSEC site-to-site VPN
- Licensing
- Monitoring
- Memory, CPU & Syslog

Note that IPV6 is not currently supported for the REST API. The Cisco CSR 1000V only supports the REST APIs over an HTTPS connection.

For more information, see the *Cisco CSR 1000V Series Cloud Services Router REST API Management Reference Guide*.

Additional Cisco IOS XE Technologies Supported in Cisco IOS XE 3.10S

The following Cisco IOS XE technologies are supported on the Cisco CSR 1000V Series Cloud Services Router beginning in Cisco IOS XE 3.10S:

- Overlay Transport Virtualization (OTV)
- Virtual Private LAN Service (VPLS)

New Cisco IOS XE Software Features in Cisco IOS XE 3.10S

This section describes new features in Cisco IOS XE 3.10S that are supported on the Cisco CSR 1000V Series Cloud Services Router and on other platforms.

- New Cisco IOS XE Software Feature in Cisco IOS XE 3.10.2S
- New Cisco IOS XE Software Features in Cisco IOS XE 3.10.0S

New Cisco IOS XE Software Feature in Cisco IOS XE 3.10.2S

The following feature has been updated in the Cisco IOS XE 3.10.2 release.

- Dropping TCP Packets During Router Reboot Process in AppNav Controller Group Scenario

  For AppNav Controller Group (ACG) scenarios, a new CLI (**service-insertion acg-reload-delay**) provides a time delay before enabling WAN traffic for a router that has just rebooted. During the delay, the router drops all TCP packets passing through the WAN interface. This enables the router to synchronize flows before traffic is enabled, preventing unintended resetting of connections.

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/partner/docs/routers/access/4400/appnav/csr-asr/apnavcsr.html

New Cisco IOS XE Software Features in Cisco IOS XE 3.10.0S

- Cisco Application Visibility and Control (AVC) Support in Cisco IOS XE 3.10S:

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios/solutions_docs/avc/ios_xe3_10/avc_user_guide_iosxe3_10.html

- TrustSec SGT Handling: L2 SGT imposition and forwarding

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_cts/configuration/xe-3s/cts-sgt-handling-imp-fwd.html

- IOS-XE GTP TEID based ECMP

  For detailed information, see the following Cisco document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipswitch_cef/configuration/xe-3s/asr1000/isw-cef-load-balancing.html#GUID-8BDF5B19-7AA9-461D-9863-B56784C126D0

New Features in and Important Notes about Cisco CSR 1000V Cloud Services Routers Release 3.9S

The following sections list the new features that are supported by the Cisco CSR 1000V Cloud Services Routers for Cisco IOS XE 3.9S.

New Platform Features in Cisco IOS XE 3.9S

This section describes the new features supported on the Cisco CSR 1000V Series Cloud Services Router in Cisco IOS XE 3.9S that are specific to this platform. For more information about these features, see the *Cisco CSR 1000V Cloud Services Router Software Configuration Guide*.

Throughput-Based Licenses

Beginning in Cisco IOS XE 3.9S, Cisco CSR 1000V licenses are based on the maximum supported throughput level. You can purchase licenses to support a maximum throughput level of 10 Mbps, 25 Mbps, or 50 Mbps. For more information, see Cisco CSR 1000V Software Licenses for Cisco IOS XE 3.10Sand 3.11S and the *Cisco CSR 1000V Cloud Services Router Software Configuration Guide*.

Additional Cisco IOS XE Technologies Supported in Cisco IOS XE 3.9S

The following Cisco IOS XE technologies are supported on the Cisco CSR 1000V Series Cloud Services Router beginning in Cisco IOS XE 3.9S:

- IP Multicast
- EoMPLS
- QoS
- Application Visibility Control (AVC)
- Network Based Application Recognition (NBAR)

Additional VMware ESXi 5.0 Features Supported in Cisco IOS XE 3.9S

The following VMware ESXi 5.0 features are supported on the Cisco CSR 1000V Cloud Services Router beginning in Cisco IOS XE 3.9S:

- Host-Level High Availability
- VM-Level High Availability
- vMotion
- Distributed vSwitch
- NIC Teaming
- NIC Load Balancing
- Mount or Pass Through of USB Storage

New and Changed CLI Commands

The following CLI commands specific to the Cisco CSR 1000V have been added in Cisco IOS XE 3.9S:

- **platform hardware throughput level**
- **show platform hardware throughput level**

The following CLI command specific to the Cisco CSR 1000V has been deprecated in Cisco IOS XE 3.9S:

- **license feature csr**

New Cisco IOS XE Software Features in Cisco IOS XE 3.9S

This section describes new features in Cisco IOS XE 3.9S that are supported on the Cisco CSR 1000V Series Cloud Services Router and on other platforms.

LISP Host Mobility Extended Subnet

For detailed information, see the following Cisco document:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-host-mob.html

LISP SHA-2 Support for Site Registration

For detailed information, see the following Cisco document:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-overview.html

SP Wifi: Integrated Ethernet over GRE support

For detailed information, see the following Cisco document:

http://www.cisco.com/en/US/docs/ios-xml/ios/interface/configuration/xe-3s/ir-eog.re.html

Compute and export Qos metrics to FNF records

For detailed information, see the following Cisco document:

http://www.cisco.com/en/US/docs/ios/solutions_docs/avc/ios_xe3_9/avc_config.html

Enable NBAR URI extraction for HTTP transactions for persistent connections

For detailed information, see the following Cisco document:

http://www.cisco.com/en/US/docs/ios/solutions_docs/avc/ios_xe3_9/avc_config.html

Flexible NetFlow: MPLS Support

For detailed information, see the following Cisco document:

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/xe-3s/fnf-mpls-support.html

NAT - Paired Address Pooling Support

For detailed information, see the following Cisco document:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/xe-3s/iadna t-addr-pool.html

Export PfR MC-id and class-id to FNF record

For detailed information, see the following Cisco document:

http://www.cisco.com/en/US/docs/ios/solutions_docs/avc/ios_xe3_9/avc_config.html

New Features in and Important Notes about Cisco CSR 1000V Cloud Services Routers Release 3.8S

The following sections list the new features that are supported by the Cisco CSR 1000V Cloud Services Routers for Cisco IOS XE 3.8S:

Note Cisco IOS XE 3.8S is a Controlled Availability release for the Cisco CSR 1000V Series Cloud Services Router.

New Platform Features in Cisco IOS XE 3.8S

This section describes the new features supported on the Cisco CSR 1000V Series Cloud Services Router in Cisco IOS XE 3.8S that are specific to this platform. For more information about these features, see the *Cisco CSR 1000V Cloud Services Router Software Configuration Guide*.

AppNav-XE on Cisco CSR 1000V Series

AppNav-XE on Cisco CSR 1000V Series is the solution that contains the following components:

- AppNav Controller: The component that intelligently distributes traffic from a router to services.
- WCM: WAAS Central Manager, which is used to monitor and configure the vWAAS application.

Note The WAAS service node must be running WAAS Release 5.1.x.

For more information, see the *Configuration Guide for AppNav-XE for Cisco Cloud Services Router 1000V Series*.

Cisco IOS XE Technologies Supported in Cisco IOS XE 3.8S

The following Cisco IOS XE technologies are supported on the Cisco CSR 1000V Series Cloud Services router in Cisco IOS XE 3.8S:

- IP
  - IPv4 Protocol
  - LISP
- VPN
  - FlexVPN
  - IPSec
  - DMVPN
  - EZVPN
- Services
  - NAT
- Access Control and Security

  - AAA
  - Access Control Lists (ACL)
  - IPSLA
  - L3FW
- Network Management
  - SNMP
  - Syslog
- Routing and Labeling
  - MPLS

Note The Cisco CSR 1000V supports only selected MPLS features in this release.

- Redundancy
  - HSRP

Network Management Support

Beginning in Cisco IOS XE 3.8S, the Cisco CSR 1000V supports Cisco Prime Infrastructure release 1.2. For more information, see the Cisco Prime Infrastructure documentation.

New VMware Required Setting

In Cisco IOS XE 3.8S, the Cisco CSR 1000V requires a VMware setting of 4 CPU sockets and 1 CPU core per socket.

New and Changed CLI Commands

The following CLI commands specific to the Cisco CSR 1000V have been changed in Cisco IOS XE 3.8S:

- The **serial** keyword was added to the **platform console** command.
- The **request license new-vudi** command was renamed to **request license new-udi**.

Caveats

This section provides information about the caveats in Cisco CSR 1000V Series Cloud Services Routers Release 3S. Caveats describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats. This section includes severity 1, severity 2, and selected severity 3 caveats.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

In this section, the following information is provided for each caveat:

- Symptom—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Search Tool (BST) to find select caveats of any severity. To reach the Bug Search Tool, log in to Cisco.com and go to https://tools.cisco.com/bugsearch/search. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

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

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

See the following sections.

- Caveats—Cisco IOS XE Release 3.11S
- Caveats—Cisco IOS XE Release 3.10S
- Caveats—Cisco IOS XE Release 3.9S

Caveats—Cisco IOS XE Release 3.11S

- Resolved Caveats—Cisco IOS XE Release 3.11.0S
- Open Caveats—Cisco IOS XE Release 3.11.0S

Resolved Caveats—Cisco IOS XE Release 3.11.0S

- CSCug99517

  Symptom: the CSR will continuing try to boot IOS and not complete. It will generate a kernel crash.

  Conditions: When enabling VMware FT on CSR VM and power up.

  Workaround: Don't enable VMware FT.

- CSCuh11994

  Symptom: cpp_svr crash noticed executing the command **show platform hardware cpp active infrastructure punt policer handle 1000 cpp**

  Conditions: Noticed without any feature configurations

  Workaround: None

- CSCuh18239

  Symptom: The CSR may crash when sweeping between 2 CSR's with larger 9KB MTU while inducing link reset.

  Conditions: When sending large MTU traffic, and creating link reset.

  Workaround: Avoid causing link reset repeatedly.

- CSCuh19651

  Symptom: cpp_cp_svr process on a CSR1000v router crashes.

Conditions: Crash occurs when nbar is configured on a virtual machine with less than 4GB of memory.

Workaround: When configuring nbar use at least 4GB of memory on the Virtual Machine.

- CSCuh36562

  Symptom: The CSR running on ESXi will dump trace back continuously when config the 10th VMXNET3 interface.

  Conditions: When configure the 10th VMXNET3 interface.

  Workaround: None

- CSCuh76624

  Symptom: The **show platform software object-manager f0 statistics** command shows pending-objects that do not clear after making configuration changes (or potentially on system boot).

  Conditions: Can occur on the CSR1000V or ISR4400X platforms with large scale configurations.

  Workaround: No workaround

- CSCui05390

  Symptom: The hierarchical QoS policy like the following is attached to an interface:

```
class-map match-any control-protocols
match access-group name control-protocols
match dscp cs6
class-map match-all netflow-export
match access-group name netflow-export
!
policy-map child-qos
class control-protocols
bandwidth percent 10
class netflow-export
bandwidth percent 5
set dscp cs6
class class-default
bandwidth percent 85
policy-map parent-qos
class class-default
shape average 50000000
service-policy child-qos
!
interface GigabitEthernet3
ip address 11.1.2.1 255.255.255.0
service-policy output parent-qos
```

  No traceback seen when the QoS policy is attached to the interface. However after saving configuration, then reboot the CSR, most of the times, the following traceback and error message is seen when the CSR boot up:

```
*Jul 11 22:20:58.678: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp: cpp_cp encountered an
error -Traceback= 1#f1dd138d618ceb5371e769279bde85a8 errmsg:7F2B10679000+121D
cpp_common_os:7F2B13694000+DA05 cpp_common_os:7F2B13694000+D904
cpp_common_os:7F2B13694000+19BDE cpp_bqs_mgr_lib:7F2B241E8000+1CDE6
cpp_bqs_mgr_lib:7F2B241E8000+123C9 cpp_qos_ea_lib:7F2B254FD000+108B5
cpp_qos_smc_lib:7F2B25781000+2016 cpp_common_os:7F2B13694000+11F9E
cpp_common_os:7F2B13694000+119DA cpp_common_os:7F2B13694000+1181B evlib:7F2B1266D00
*Jul 11 22:20:58.701: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image: qos hqf:
class=0.0, dpidx=6, qid=0x0:0x40000001 (p:0x40000001), dir=both directions download to
CPP failed
```

Conditions: Attaching hierarchical QoS policy to interface, save config, and reboot the CSR.

Workaround: None.

- CSCui36288

  Symptom: CRS kernel crash when adding or removing vNIC to the CSR VM from vSphere.

  Conditions: Add/remove vNIC.

  Workaround: None.

- CSCuj50874

  Symptom: CSR licensing not taking any effect Conditions: On a CSR router with 10Mbps license, we are able to send 54Mbps of traffic without any drops

  Workaround: none

- CSCuj78853

  Symptom: Crash when doing config replace with active traffic

  Conditions: With OTV active flow, when we do config replace, we observe the crash.

  Workaround: none

Open Caveats—Cisco IOS XE Release 3.11.0S

- CSCui49262

  Symptom: No characters are displayed when typed.

  Conditions: When booting up CSR with csr.cnfg.

  Workaround: Reboot the CSR.

- CSCuj45318

  Symptom: The CSR Management container hosting the REST API and Cisco Prime Network Services Controller functionalities sometimes cannot successfully pick up its IP address from the system configuration. This will result in two symptoms:

  - REST API URLs will not be reachable.
  - Cisco PNSC will report the Cisco CSR1000V as unreachable.

  Conditions: During periods of high memory usage, particular during boot up after license level change.

  Workaround: Reboot the Cisco CSR1000V.

- CSCuj95999

  Symptom: The **call-home reporting contact xxx** command can't restore SCH report data of TAC profile.

  Conditions: Issue **no reporting smart-call-home-data** under CiscoTAC-1 profile.

  Workaround: Issue **reporting smart-call-home-data** under CiscoTAC-1 profile.

Caveats—Cisco IOS XE Release 3.10S

- Resolved Caveats—Cisco IOS XE Release 3.10.2S
- Resolved Caveats—Cisco IOS XE Release 3.10.1S

Resolved Caveats—Cisco IOS XE Release 3.10.2S

- CSCug63839

  Symptom: The Cisco 7301 router running c7301-advipservicesk9-mz.152-4.M3 experiences a memory leak in the Crypto IKMP process particularly on the crypto_ikmp_config_send_ack_addr function.

  Conditions: This symptom occurs when running the Cisco 7301 router and connecting EasyVPN through it.

  Workaround: Reload the router over a period of time.

- CSCuh35993

  Symptom: create an RRI route for deny ACL lines in the crypto map

  Conditions: 15.x code and L2L ipsec tunnel

  Workaround: None

- CSCui06926

  Symptom: Initiator sends identity certificate based on “ca trustpoint” under the isakmp-profile. However, the responder does not do this. Instead it gets the identity certificate from the *first* trustpoint (out of the list of trustpoints) based on peer's cert_req payload in MM3.

  Conditions: This symptom is observed under the following conditions: 1. IKEv1 with RSA-SIg Authentication, where each Peer has two certificates issued by the same CA. 2. Each Peer has isakmp profiles defined that match on certificate-map and have “ca trustpoint” statements with self-identity as fqdn.

  Workaround: There is no workaround. At this point, responder does not have control over selecting the right certificate.

- CSCui84532

  Symptom: RP is again fragmenting it.

  Conditions: Giant pkts are sent from SPA after LAF.

  Workaround: No work around.

- CSCui85371

  Symptom: Ikev2 session is NOT coming UP

  Conditions: Ikev2 session is NOT coming UP Loopback to loopback ping is not going through.

  Workaround: NO

- CSCuj02503

  Symptom:'Internal_service' license state shows as 'Active, Not In Use' even after its expiry. The system Linux Shell cannot be accessed upon expiry of the 'Internal_service' 1 Day license which is expected. However if an new 1 Day license is installed again, the license state comes up as 'Active, In Use' but Linux Shell cannot be accessed. Conditions:Install 1 Day 'Internal_service' license. Let the license expire then install another 1 Day 'Internal_service' license.

  Workaround: Configure and Unconfigure the 'platform shell' configuration command to recover the license to proper working state.

```
Router#config terminal
Router(config)#platform shell
Router(config)#no platform shell
Router(config)#platform shell
```

Now the System Linux Shell would be accessible.

- CSCuj02519

  Symptom: Chunk memory leak in Crypto Proxy

  Conditions: This is only seen with IPSEC HA configured

  Workaround: None at this time.

- CSCuj31165

  Symptom: crpcipSecGlobalActiveTunnels is incrementing endlessly.

  Conditions: crpcipSecGlobalActiveTunnels OID does not decrements when the current active tunnel is removed.

  Workaround: no work around.

- CSCuj71234

  Symptom: Tracebacks with the following signature "%QFPOOR-4-LOWRSRC_PERCENT" are seen on the console with negative percentage complaining of resource depletion.

  Conditions: These tracebacks are usually seen on a clean-up operation performed on a router i.e manual removal of all configs. But it's not limited to only this operation and could be seen with router configuration as well.

  Workaround: None.

  Further Problem Description: Error messages with “-ve” percentage values of resource depletion are incorrectly being printed on the console. It's safe to ignore them as the router is not under any duress. Moreover these traces don't cause any operational impact. It should be noted however that if such tracebacks are reported with “+ve” percentage values of resource depletion, then it's an altogether different issue. In such a case, the system may be under duress and inspection of the router configs and it's operational state is required.

- CSCuj84219

  Symptom: Error messages shown on KS after SW upgrade to 15.2(4)M. Whenever a GM with multiple GDOI groups registers, an error message is logged on the respective KS: Oct 4 11:31:28.477 CEST: %CRYPTO-6-IKMP_NO_ID_CERT_FQDN_MATCH: ID of ce-de-xxxxx.wan.domain.net (type 2) and certificate fqdn with ce-de-xxxxx

  Conditions: Multiple GDOI groups with different GETVPN local-addresses configured on GM. GM/KS are ISR G2 routers running on 15.2(4)M code.

  Workaround: Configure “crypto isakmp identity dn”, i.e. set the ISAKMP identity to the distinguished name (DN) of the router certificate.
  http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c4.html#wp1060149

- CSCul20010

  Symptom: The user will see the system shaping to too low a rate when a tunnel moves to a faster interface, and shaping to too high a rate when a tunnel moves to a slower interface.

  Conditions: Upon a dynamic move of a tunnel to a link with a different speed and the QoS configuration option “shape average percent” has been applied, then rates are not automatically re-calculated.

Workaround: The workaround to this issue is to avoid “shape average percent” when possible. If not possible, then after a tunnel moves occurs modify the shaping percent by plus or minus 1 percent, and then restore to original value because this forces recalculation of the shaping rate.

- CSCul02627

  Symptom: UEA: Log files are not generated with PTP configs

  Conditions: Configure RSP2 as the slave and RSP1 as the master Go to shell using “request platform software system shell” cd /tmp/rp/trace ls -ltr Notice that the log files related to PTP aren't present.

  Workaround: Reload of RSP2

- CSCul04434

  Symptom: Given a GETVPN GM that is configured with an ipv6 crypto map, if that crypto map is applied to two interfaces (one common identity, e.g. loopback) and if certain configuration operations are performed, the GM will loose connectivity to the ipv6 group. If the GM has dual-stack interfaces with both an ipv4 and an ipv6 crypto map. The IPv4 GETVPN functionality will not be affected while triggering the event documented in this defect.

  Conditions: Performing configuration operations that follow the patterns described below : 0. IPv6 Crypto Map applied to two interface (E0/0 and E2/0, lets call them Primary and Secondary) At this stage all works well IPv6 traffic is encrypted between two test GMs.

  1. Shut down Secondary interface (E2/0) Result, no change in functionality GM can still exchange encrypted IPv6 traffic with peers.

  2. Remove the ipv6 crypto map from the Primary interface (E0/0, while E2/0 is in admin shutdown state). Result, IPv6 traffic is sent out in clear text

  3. Re-apply crypto map to the Primary interface (i.e. E0/0) Result, no change, packets are still being sent out in clear text, even though GDOI sees the E0/0 interface as associated with the cry map and group.

  4. Remove the crypto map from the Secondary interface which is still in shutdown state Result : No change in the behavior

  5. Remove and re-apply the crypto map on the Primary interface Result : GM re-registers

  Workaround: Remove the ipv6 crypto map from the Secondary Interface before shutting it down.

- CSCul15647

  Symptom: Classification by ACL in QoS is broken when using it with IPSec tunnel.

  Conditions: -use ACL for classification in policy-map and apply a QoS to physical interface -qos pre-classify is configured under IPSec tunnel

  Workaround: apply a QoS to IPSec tunnel

- CSCul39211

  Symptom: With an IOS router set as an EZVPN client, with either interactive (CLI) or HTTP-Intercept authentication enabled, if the user does not enter in proper credentials within 10 seconds, the router will resend AM3 to the EzVPN server. This causes a retransmission storm to trigger and quickly tear down the tunnel, which causes the authentication to fail.

  Conditions: IOS router acting as EzVPN client

  Workaround: 1) Have users enter credentials within 10 seconds of login prompt. 2) Save credentials on router so users don't need to enter them every time. 3) Downgrade to 15.1(4)M5 or earlier

- CSCul95089

  Symptom: AAA sessions are lingering for old connections.

Conditions: Running Flex VPN server with accounting, clients are identified by email id

Workaround: none

Further Problem Description: Accounting sessions are not cleared when a client does reconnect from a different IP upon reception and parsing of the IKEv2 Initial Contact payload

- CSCum14041

  Symptom: QFP error logs not displayed on IOS console.

  Conditions: IOS-XE 3.10/15.3(3)S and forward releases.

  Workaround: None.

Resolved Caveats—Cisco IOS XE Release 3.10.1S

- CSCuh07934

  Symptom: No error-message for reason with restapi GET interface failure.

  Conditions: Restapi GET interface on CSR 1000V interface which has ipv6 address configured.

  Workaround: None

- CSCuc41531

  Symptoms: Forwarding loop is observed for some PfR-controlled traffic. Conditions: This symptom is observed with the following conditions: - Traffic Classes (TCs) are controlled via PBR. - The parent route is withdrawn on selected BR/exit.

  Workaround: This issue does not affect configured or statically defined applications, but only affects learned applications so this can be used as one workaround. Another option is to issue shut/no shut on PfR master or clear the related TCs with the **clear pfr master traffic-class** ... command (this fixes the issue until the next occurrence).

- CSCud49546

  Symptom: RP crashes with punted fragment-bit set multicast packet.

  Conditions: Fragment bit is set in the multicast packet

  Workaround: None

- CSCue89779

  Symptom: A FlexVPN spoke configured with an inside VRF and front-door VRF may have problems with spoke-to-spoke tunnels if they are not the same. During tunnel negotiation, two Virtual-access interfaces are created (while only one is needed), the one in excess may fail to cleanup correctly. As a result, the routes created by NHRP process may lead to loss of traffic, or traffic may continue to flow through the Hub.

  Conditions: This symptom occurs when the VRF used on the overlay (IVRF) and the VRF used on the transport (FVRF) are not the same.

  Workaround: There is no workaround.

- CSCuf56842

  Symptom: A reload may occur while using **show oer** and **show pfr** commands via SSH.

  Conditions: This symptom is observed when the show pfr master application detail command is used via SSH.

  Workaround: There is no workaround.

- CSCug69107

Symptom: Crypto session does not comes up in EZVPN.

Conditions: This symptom is observed when a Crypto session is being established.

Workaround: There is no workaround.

- CSCug99771

  Symptom: OSPF N2 default route missing from Spoke upon reloading Hub. Hub has a static default route configured and sends that route over DMVPN tunnel running OSPF to spoke. When hub is reloaded, the default route is missing on Spoke. NSSA-External LSA is there on Spoke after reload, but the routing bit is not set. Hence, it is not installed in RIB on Spoke.

  Conditions: Default originated using command **area X nssa default-information-originate**.

  Workaround: Removing & re adding **area X nssa default-information-originate** on Hub resolves the issue.

- CSCuh32177

  Symptom: The **no passive-interface** command will be added automatically after configuring the **ipv6 enable** command on the interface even though the **passive-interface default** command is configured for OSPFv3.

  ```
  (config)#interface FastEthernet0/2/0
  (config-if)#ipv6 enable (
  config-if)#end #sh run | sec ipv6 router ospf ipv6 router ospf 100 router-id 10.1.1.1
  passive-interface default no passive-interface FastEthernet0/2/0 <<< Added
  automatically. ---
  ```

  Conditions: This symptom occurs when the **passive-interface default** command is configured for OSPFv3.

  Workaround: Adjust the configuration manually. In this example it would be **passive-interface FastEthernet0/2/0**.

- CSCuh43027

  Symptom: Prefixes withdrawn from BGP are not removed from the RIB, although they are removed from the BGP table.

  Conditions: A withdraw message contains more than one NLRI, one of which is for a route that is not chosen as best. If deterministic med is enabled, then the other NLRI in the withdraw message might not eventually be removed from the RIB.

  Workaround: Forcibly clear the RIB.

  Further Problem Description: This issue may also occur if BGP PIC is enabled and the withdraw message contains a route that is currently serving as a backup path.

- CSCuh94035

  Symptom: A watchdog timeout crash occurs.

  Conditions: This symptom occurs when DMVPN and IPv4/IPv6 EIGRP are configured. A crash occurs while DUAL is updating the EIGRP topology table.

  Workaround: There is no workaround.

- CSCuh97129

  Symptom: Losing EIGRP Extended communities on BGP L3VPN route.

  Conditions: This symptom is observed when Remote PE-CE connection is brought down and only backup EIGRP path remains in the BGP table.

  Workaround: Clearing the problem route in the VRF will resolve the issue.

- CSCui07997

  Symptom: Route over OSPFv2 sham-link shows two next hop.

  Conditions: This symptom is observed when the route entry is ECMP route between the sham-link and another path.

  Workaround: Break ECMP by adjusting the OSPF cost.

- CSCui29499

  Symptom: ISIS going into INIT state.

  Conditions: BFD flap leads to ISIS adjacency not coming up if the following conditions are true: 1.) In P2P mode only 2.) when local node supports RFC6213 and its remote neighbor does not support RFC6213 3.) The P2P link is down and adjacency is deleted on the remote neighbor and up again before the adjacency hold down timer expires on the local node that has the RFC6213 support.

  Workaround: Any of the following work around will work. - Remove BFD on 903, wait for ISIS to come up and configure BFD again - Shut and no shut the interface on the local node with RFC6213 Or - Not to use P2P link at all

- CSCui89069

  Symptom: ISIS Flap on performing SSO .

  Conditions: with **nsf ietf** configured and one or more loopbacks configured as passive interfaces

  Workaround: Two workarounds are available: 1)use **nsf cisco** or 2) Continue to use **nsf ietf** but configure **ip router isis** *process_name* on the loopback interfaces.

Resolved Caveats—Cisco IOS XE Release 3.10.0S

- CSCud23158

  Symptom: On the Cisco CSR1000v an unexpected reset may occur when sending IPv4 small packet traffic at a high rate.

  Conditions: This is intermittently seen with a basic CEF configuration passing bi-directional 64 Byte traffic near 100% Gigabit Ethernet line-rate.

  Workaround: None

- CSCud71606

  Symptom: The LSMPI Tracebacks errors are seen while clearing IP routes multiple times.

  Conditions: This symptom is observed under the following conditions:

  - Configuring OSPF.
  - Has more than 1000 OSPF neighbors, which will make OSPF LSU packet get fragmented.
  - Clear ip ospf process * and OSPF will send an LSU packet, which triggers this error message.

  Workaround: None.

- CSCue39542

  Symptom: Tunnel interface states down and fail to carry traffic.

  Conditions: The tunnel interface stays down after the tunnel stay flaps. Can be from issuing “shut” and “no shut” commands manually, or the physical port state flaps. And the tunnel state might stay down forever after the event.

  Workaround: Delete and recreate the tunnel interface with the same config will bring this tunnel back to up state.

- CSCue41031

  Symptom: Extra flow is shown in **show crypto session** command.

  Conditions: None.

  Workaround: None.

- CSCue95542

  Symptom: A crash was observed after configuring ethernet CFM on the router. The crash occurred in the linux_iosd process.

  Conditions: The crash was seen on the Cisco ISR4400 and the Cisco CSR1000v.

  Workaround: Do not configure CFM.

- CSCuf09252

  Symptom: Incorrect error message is seen when giving no parameter-map type inspect-global.

  Conditions: Parameter-map type inspect global should be defined.

  Workaround: None.

- CSCuh20338

  Symptom: ucode crash @ ipv4_ipsec_tunnel_input

  Conditions: Bringup 10 FlexVPN sessions on Cisco CSR 100V.Workaround: Enter the **no ip source-route** command.

- CSCuh70383

  Symptom: The Cisco CSR 1000V is deployed from the OVF template, powered up until completion of the 1st time boot process, then powered down and a new vNIC is added while the router is offline. After the router is powered up again, the new interfaces are recognized but the Cisco CSR 1000V VM is observed at operating with 100% CPU usage. The router stays at 100% CPU as long as the newly added interface is in admin shutdown state. CSR CPU usage revert to normal once the interface is admin 'no shutdown'. Not all interface additions will result in this condition.

  Conditions: When adding a new vNIC to the Cisco CSR 1000V.

  Workaround: After the new interface is added, administer the **no shutdown** to the interface.

Open Caveats—Cisco IOS XE Release 3.10.0S

- CSCue33225

  Symptom: The **sh plat hard qfp act dat infr sw-hqf** output is truncated.

  Conditions: When 5 Gi interfaces are defined, the output is truncated

  Workaround: Use less than 5 Gi interfaces.

- CSCue75176

  Symptom: IDFW is not working for sgt replaced because of policy static sgt <sgt-num> command.

  Conditions: Configure policy static sgt <sgt-num> command on ingress interface and in FW do match for same sgt number given in this CLI.

  Workaround: None.

- CSCuf28574

  Symptom: Cisco CSR1000V running on XEN will see significantly lower throughput than on other hypervisors, i.e. ESXi.

Conditions: Cisco CSR1000v running on XEN Server 6.02

Workaround: None.

- CSCug13606

  Symptom: Gigabit Ethernet interface counters show a value near 2 to the 64th.

  Conditions: Occurs on a Cisco CSR1000V router using VMXNET3 driver after an Etherchannel interface is configured.

  Workaround: Performing "clear counters" will reset the counter to zero.

- CSCug51917

  Symptom: Hot removal of an interface not possible in the case of CSR 1000V [installed on an ESXi server].

  Conditions: Issue seen when try to remove an interface from the Cisco CSR 1000V router when it is UP.

  Workaround: None.

- CSCuh12291

  Symptom: RESTAPI interface discovery will fail.

  Conditions: Having ipv6 address configured on interface and do RESTAPI GET interface.

  Workaround: None

- CSCuh28560

  Symptom: After booting up, two VMs came up with no installed licenses. Could not recover the licenses since the UDI of the VMs changed.

  Conditions: Reset all Cisco CSR 1000V VMs running on a server (4:1 CPU oversubscription). All VMs are 4 vCPU with 4 GB RAM and 3 NICs each.

  Workaround: Do not oversubscribe.

- CSCuh49807

  Symptom: IPsec transform set with esp-md5-hmac is not supported in this release. When esp-md5-hmac is used, though the IPsec tunnel is established, traffic can not pass through the tunnel. Inbound traffic will be dropped with HMAC error. Outbound traffic will reach to the peer, but will be dropped by the peer with HMAC error.

  The following error message is displayed:

  ```
  %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:000 TS:00000002356612773534
  %IPSEC-3-HMAC_ERROR: IPSec SA receives HMAC error, DP Handle 5, src_addr 60.0.0.2,
  dest_addr 60.0.0.1, SPI 0xb98e9ee1
  ```

  Conditions: Whenever esp-md5-hmac is used in an IPsec transform set.

  Workaround: Use esp-sha-hmac, not esp-md5-hmac.

- CSCuh73332

  Symptom: Can show "Last reload reason: <NULL>"

  Conditions: CPP crash on CSR

  Workaround: None

- CSCui12606

  Symptom: If Gi1 interface does not exist on the CSR when the CSR boots up, the following error message is logged:

```
*Jul 16 14:57:17.598: %IOSXE-4-PLATFORM: R0/0: kernel: TIPC: Bearer <eth:Gi1>
rejected, enable failure (19)
*Jul 16 14:57:18.722: %PMAN-3-PROCHOLDDOWN: F0: pman.sh:  The process
wui-tipc-launch.sh has been helddown (rc 255)
```

The Gi1 interface (usually vnic2 of the CSR VM) could disappear from CSR for any one of the following reasons:

1) the vNIC is deleted from vSphere then the CSR is rebooted

2) the MAC address of the vNIC is changed from vSphere

Conditions: Gi1 interface does not exist on the CSR.

Workaround: If the CSR has multiple vNICs, use the 'clear platform software vnic-if nvtable' command to remap the vNICs to interfaces mapping, then reboot the CSR. Note that the command might remap the interfaces not in the order shown on vSphere for the CSR VM. Use with care.

- CSCui41279

  Symptom: When the CSR1000V boots in premium mode, cannot configure throughput level or install a new premium throughput level license. Throughput will be set to 2500 kbps.

  Conditions: CSR boot in premium mode with premium license.

  Workaround: Reload the router.

Caveats—Cisco IOS XE Release 3.9S

Resolved Caveats—Cisco IOS XE Release 3.9.2S

None.

Resolved Caveats—Cisco IOS XE Release 3.9.1S

- CSCuc11849

  Symptom: Packets of smaller lengths (less than 100 bytes) may be dropped occasionally when a shaper is configured.

  Conditions: This issue happens when a shaper is configured on CSR1000V and traffic consisting of smaller packet lengths (less than 100 bytes) are sent below the configured shape rate.

  Workaround: There is no known workaround.

- CSCue04941

  Symptom: When CSR1000V is being used as a VPN gateway and BFD session, the number of stable BFD sessions is lower than expected.

  Conditions: When CSR1000V is being used as a VPN gateway and BFD session, the number of stable BFD sessions is lower than expected.

  Workaround: None.

- CSCuf29962

  Symptom: Getting aggressive alert is seen when no alert is set.

  Conditions: ZBFW is on and alert is seen after disabling the parameter-map type inspect global and clearing drops.

  Workaround: None

- CSCuf86458

  Symptom: Crash kernel does not work on ESXi.

  Conditions: When main kernel crashes, it does not dump core.

  Workaround: None

Open Caveats—Cisco IOS XE Release 3.9.0aS

- CSCuf51492

  Symptom: All of the IPSEC sessions didn't come up after ISAKMP Rekey

  Conditions: Noticed in a scaled DMVPN topology.

  Workaround: None

Resolved Caveats—Cisco IOS XE Release 3.9.0aS

- CSCsr10335

  Symptoms: A router loses its default gateway during autoinstall.

  Conditions: This issue was seen on Cisco IOS Release 12.4(15)T5, but should affect every Cisco IOS version.

  Workaround:

  1. Manually do a **shut** followed by a **no shut** on the interface.

  2. Create an EEM script, for example:

```
event manager applet Check-Default-Route event syslog pattern "CNS-3-TRANSPORT:
CNS_HTTP_CONNECTION_FAILED"

 action 1.0 cli command enable
 action 1.1 cli command config term
 action 1.2 cli command interface GigabitEthernet0/0<
 action 1.3 cli command shut
 action 1.4 cli command no shut
 action 1.5 cli command end
 action 1.6 cli command write ! end
```

  3. In the network configuration, configure **ip address dhcp** for the interface which is supposed to get the default gateway from DHCP.

- CSCuc17133

  Symptom: The CSR router would crash at IPSec code if a DMVPN session is up and running for some time.

  Conditions: Usually happens within an hour. No traffic is needed.

  Workaround: None.

- CSCuc45115

  Symptoms: EIGRP flapping is seen continuously on the hub. A crash is seen at nhrp_add_static_map.

  Conditions: This symptom is observed in the case where there are two Overlay addresses of a different Address Family on the same NBMA (such as IPv4 and IPv6 over Ipv4). This issue is observed after shut/no shut on the tunnel interface, causing a crash at the hub. A related issue is also seen when there is no IPv6 connectivity between the hub and spoke, causing continuous EIGRP flapping on the hub.

  Workaround: There is no known workaround.

- CSCuc99788

  Symptom: ERSPAN traceback

  Conditions: Configured 2k sub-interfaces.

  Workaround: None

- CSCud02391

  Symptoms: The EIGRP routes do not come up after removing and reenabling the tunnel interface.

  Conditions: This symptom is observed when EIGRP routes do not populate properly.

  Workaround: There is no workaround.

- CSCud03863

  Symptom: ESP crashes on CSR

  Conditions: Crash occurs when sending traffic through a non gig 0 interface

  Workaround: No workaround as this is caused by unsupported CPUs with missing features. As per the data sheet (http://www.cisco.com/en/US/prod/collateral/routers/ps12558/ps12559/data_sheet_c78-705395.pdf), the CPU requirement is “Intel Nehalem or AMD Barcelona CPU with clock frequency 1.8GHz” or higher.

- CSCud23158

  Symptom: On the CSR1000V an unexpected reset may occur when sending IPv4 small packet traffic at a high rate.

  Conditions: This is intermittently seen with a basic CEF configuration passing bi-directional 64 Byte traffic near 100% Gigabit Ethernet line-rate.

  Workaround: None

- CSCud67970

  Symptom: Provisioned QoS service is not honored.

  Conditions: When fair-queue is removed from the class on-the-fly, the rates, i.e., bandwidth and shape, are no longer configured in the hardware.

  Workaround: Remove the fair-queue class and re-add it without fair-queue.

- CSCud71606

  Symptom: LSMPI Tracebacks/Errors seen while clearing IP routes multiple times.

  Conditions: ASR- GIG-------IXIA >> 2K vlans on GIGE and IXIA subi-intfs >> OSPF neighbour hood was properly achieved with 1000 Vlans

  Workaround: None

- CSCud93920

  Symptom: QFP errors on applying AVC to MPLS interfaces.

  Conditions: AVC is not supported on an MPLS interface so this is a misconfiguration.

  Workaround: Not applicable.

- CSCue36106

  Symptom: This warning message would be emitted on the IOS console on Cisco CSR1000V installed on the VMWARE ESXi with VMXNET3 network adapter.

  Conditions: When the Cisco CSR1000V is over-subscribed and ESXi is not be able to handle the traffic.

  Workaround: This is a warning message and VMXNET3 driver recovers from this condition.

  Make sure that the Cisco CSR1000V is not over-subscribed to avoid this.

- CSCue39542

  Symptom: Tunnel interface stays down and fails to carry traffic.

  Conditions: The tunnel interface stays down after the tunnel stay flaps. Can be from issuing **shut** and **no shut** commands manually, or the physical port state flaps. And the tunnel state might stay down forever after the event.

  Workaround: Deleting and recreating the tunnel interface with the same configuration will bring this tunnel back to up state.

Related Documentation

Platform-Specific Documents

For information about installing and configuring the Cisco CSR 1000V, see the following documents:

- *Cisco CSR 1000V Series Cloud Services Router Software Configuration Guide*
- *Cisco CSR 1000V Series Cloud Services Router Deployment Guide for Amazon Web Services*
- *Cisco CSR 1000V Series Cloud Services Router REST API Management Reference Guide*

Cisco IOS Software Documentation Set

The Cisco IOS XE 3S software documentation set consists of Cisco IOS XE 3S configuration guides and Cisco IOS command references. The configuration guides are consolidated platform-independent configuration guides organized and presented by technology. There is one set of configuration guides for the Cisco IOS release train and another for the Cisco IOS XE 3S release train. However, there is only one set of command references because they are platform independent—Cisco IOS command references support all Cisco platforms that are running any Cisco IOS or Cisco IOS XE software image.

See http://www.cisco.com/en/US/products/ps11174/tsd_products_support_series_home.html

Note All content included in Cisco IOS configuration guides is shared with and included in the Cisco IOS XE 3S configuration guides. As a result, some information for features introduced as part of Cisco IOS XE 3S may also be displayed in Cisco IOS configuration guides.

Information in the configuration guides often includes related content that is shared across software releases and platforms. Some features referenced in these configuration guides may not be supported by Cisco IOS XE 3S or by the Cisco CSR 1000V Series Cloud Services Routers.

Additionally, you can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on cisco.com is not required.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.