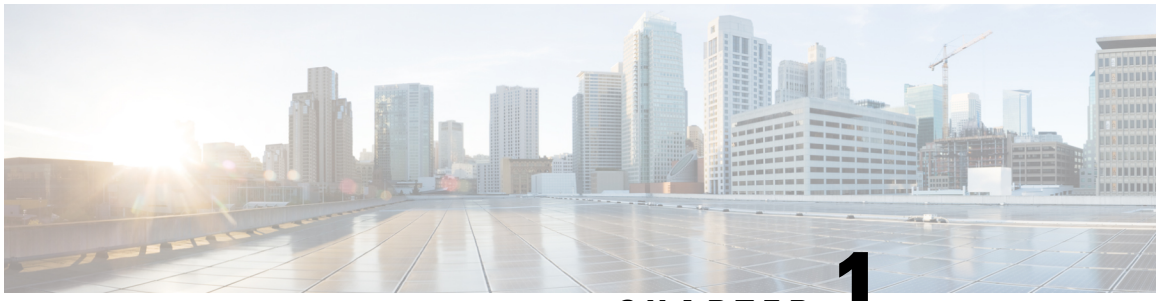
Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-31

Last Modified: 2022-09-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Introduction

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

This document provides information about the IOS XE software release for the Cisco NCS 4201 and Cisco NCS 4202 beginning with Cisco IOS XE Release 3.18SP.

Documentation Updates

Cumulative Configuration Guides for Cisco IOS XE 16 Release Series

From Cisco IOS XE Everest 16.5.1 to Cisco IOS XE Gibraltar16.12.1, technology configuration guides were published for each release and contained information specific to only that release.

For example, the *MPLS Configuration Guide Cisco IOS XE Everest 16.5.x* contained information specific to only the Cisco IOS XE Everest 16.5.x release.

However, all technology configuration guides will now contain information about all features supported by all releases of the Cisco IOS XE 16 Series.

For example, the *MPLS Configuration Guide Cisco IOS XE 16 Series* is republished and contains information about all MPLS features supported by releases from *Cisco IOS XE Everest 16.5.x to Cisco IOS XE Gibraltar 16.12.x*.

The following documents will help identify release features supported in every release:

- Feature History – A new chapter in all configuration guides. This chapter lists the features and the release in which the features are introduced or updated.
- Release Notes – This document continues to be specific for each release and carries information about the feature supported in that release.
- Feature Compatibility Matrix – A cumulative feature-release matrix, which is available on Cisco.com.
  - Feature Compatibility Matrix for NCS 4201 and NCS 4202
  - Feature Compatibility Matrix for NCS 4206 and NCS 4216

Cisco NCS 4201 and Cisco NCS 4202 Overview

The Cisco NCS 4201 and NCS 4202 Network Convergence Systems are full-featured, compact one-RU high converged access platforms designed for the cost-effective delivery of TDM to IP or MPLS migration services. These temperature-hardened, high-throughput, small-form-factor, low-power-consumption systems are optimized for circuit emulation (CEM) and business applications. NCS 4201 and NCS 4202 chassis allow service providers to deliver dense scale in a compact form factor and unmatched CEM and Carrier Ethernet (CE) capabilities. They also provide a comprehensive and scalable feature set, supporting both Layer 2 VPN (L2VPN) and Layer 3 VPN (L3VPN) services in a compact package .

For more information on the Cisco NCS 4201 Chassis, see the Cisco NCS 4201 Hardware Installation Guide.

For more information on the Cisco NCS 4202 Chassis, see the Cisco NCS 4202 Hardware Installation Guide.

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.

Hardware Supported

NCS4201 is a fixed router and does not have any field replaceable units.

The following table lists the hardware supported for Cisco NCS 4202 chassis.

Chassis	Supported Interface Modules	Part Numbers
NCS 4202	8 port T1/E1 CEM Interface Module	NCS4200-8E1T1-CE
	1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 ports T1/E1 + 4 ports T3/E3	NCS4200-3GMS
	8-Port 1GE RJ45 and 1-Port 10GE SFP+ module	NCS4200-1T8LR-PS

Determining the Software Version

You can use the following commands to verify your software version:

- Consolidated Package— **show version**
- Individual sub-packages—**show version installed** (lists all installed packages)

Table 1: ROMMON Version

Release Version	ROMMON Version
16.12.8	• NCS4201—15.6(48r)S • NCS4202—15.6(46r)S
16.12.7	• NCS4201—15.6(48r)S • NCS4202—15.6(46r)S
16.12.6	• NCS4201—15.6(48r)S • NCS4202—15.6(46r)S
16.12.5	• NCS4201—15.6(32r)S • NCS4202—15.6(24r)S

Bundled FPGA Versions

The following are HoFPGA versions bundled in the IOS:

- NCS4201—0X00030015
- NCS4202
  - BFD—0X0003001c

- Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—0x10050071

The following are HoFPGA versions bundled in IOS for 16.12.8, 16.12.7 and 16.12.6 releases:

- NCS 4201— 0X00040019
- NCS 4202
  - BFD—0X0003001b
  - Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—NA

Limitations and Restrictions on the Cisco NCS 4201 and Cisco NCS 4202 Series

- The **default** *command-name*command is used to default the parameters under that interface. However, when speed is configured on the interface, the following error is displayed:

  ```
  Speed is configured. Remove speed configuration before enabling auto-negotiation
  ```

- VCoP/TSoP smart SFPs are not supported.
- Virtual services should be deactivated and uninstalled before performing replace operations.
- IPSec is not supported on the Cisco NCS 4201 and Cisco NCS 4202 routers.
- On Cisco NCS 4202 Series, the following restrictions apply for IPSec:
  - Interface naming is from right to left. For more information, see the Cisco NCS 4200 Series Software Configuration Guide
  - Packet size greater than 1460 is not supported over IPsec Tunnel.
  - Minimal traffic drop might be seen for a moment when higher rate traffic is sent through the IPsec tunnels for the first time.
  - IPsec is only supported for TCP and UDP and is not supported for SCTP.

Field Notices and Bulletins

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

- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

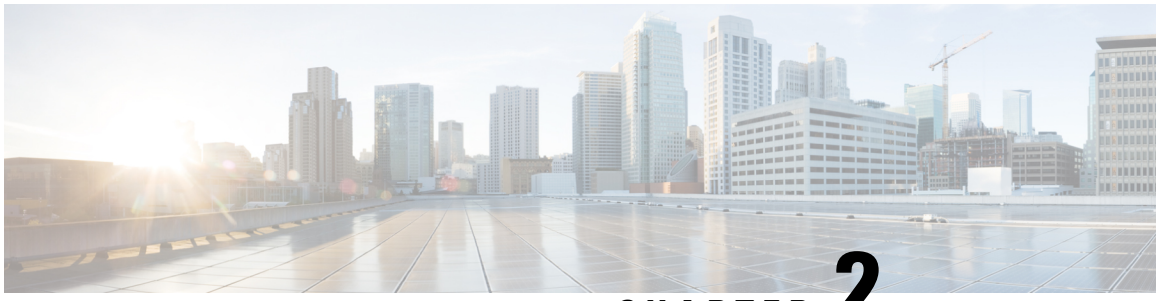
MIB Support

To view supported MIB, go to http://tools.cisco.com/ITDIT/MIBS/MainServlet.

Accessibility Features in the Cisco NCS 4201 and Cisco NCS 4202 Series

For a list of accessibility features in Cisco NCS 4201 and Cisco NCS 4202 Series, see the Voluntary Product Accessibility Template (VPAT) on the Cisco website, or contact accessibility@cisco.com.

All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.



CHAPTER 2

New Features

This chapter describes the new hardware and software features that are supported on the Cisco NCS 4201 and Cisco NCS 4202 Series routers.

New Software Features in Cisco IOS XE Gibraltar 16.12.8

There are no new software features for this release.

New Hardware Features in Cisco IOS XE Gibraltar 16.12.8

There are no new hardware features for this release.

New Software Features in Cisco IOS XE Gibraltar 16.12.7

There are no new software features for this release.

New Hardware Features in Cisco IOS XE Gibraltar 16.12.7

There are no new hardware features for this release.

New Software Features in Cisco IOS XE Gibraltar 16.12.6

There are no new software features for this release.

New Hardware Features in Cisco IOS XE Gibraltar 16.12.6

There are no new hardware features for this release.

New Software Features in Cisco IOS XE Gibraltar 16.12.5

There are no new features for this release.

New Hardware Features in Cisco IOS XE Gibraltar 16.12.5

There are no new features for this release.

New Software Features in Cisco IOS XE Gibraltar 16.12.4

- **Configurable Y.1564 Service Activation Frame Sizes and EMIX Support**

  Enterprise traffic (EMIX) packet size (default abceg pattern) is supported. For EMIX traffic, ITU-T Rec. Y.1564 packet sizes of 64, 128, 256, 1024, and 1518 bytes are supported.

  For more information, see the IP SLAs Configuration Guide, Cisco IOS XE Gibraltar 16 (Cisco NCS 4200 Series).

- **SADT Overhead Accounting**

  FPGA measures the following parameters for SADT:

  - Throughput
  - Frame Loss
  - Jitter
  - Delay

  FPGA has the capability to generate and measure only 1Gbps traffic rate and hence maximum throughput cannot be achieved. To overcome this limitation, use the **platform y1564 shadow-session-enable** command to replicate the packets 10 times in FPGA.

For more information, see IP SLAs Configuration Guide, Cisco IOS XE Gibraltar 16 (Cisco NCS 4200 Series).

New Hardware Features in Cisco IOS XE Gibraltar 16.12.4

There are no new features for this release.

New Software Features in Cisco IOS XE Gibraltar 16.12.3

There are no new features for this release.

New Hardware Features in Cisco IOS XE Gibraltar 16.12.3

There are no new features for this release.

New Software Features in Cisco IOS XE Gibraltar 16.12.2a

There are no hardware features for this release.

New Hardware Features in Cisco IOS XE Gibraltar 16.12.2a

There are no hardware features for this release.

New Software Features in Cisco IOS XE Gibraltar 16.12.1

- **Segment Routing uLoop Avoidance**

  The Segment Routing uLoop Avoidance feature prevents the occurrences of microloops during network convergence after a link-down event or link-up event.

  For more information, see the Segment Routing Configuration Guide, Cisco IOS XE Gibraltar 16.12.x (Cisco NCS 4200 Series).

- **Transparent PDH over Packet Smart SFP**

  The TPoP smart SFP now transparently encapsulates the T1 stream into a SAToP packet for pseudowire transport over the PSN.

  For more information on TPoP smart SFP, see the Time Division Multiplexing Configuration Guide, Cisco IOS XE Gibraltar 16.12.x (Cisco NCS 4200 Series).

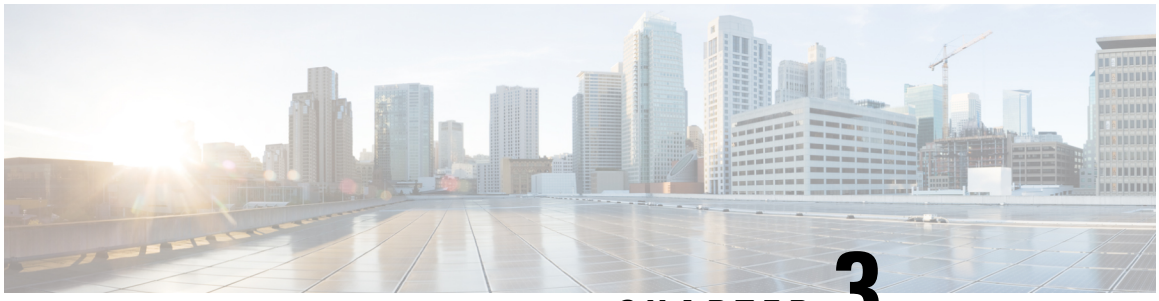
- **Y.1564 10G internal mode**

Y.1564 is an Ethernet service activation test methodology and is the standard for turning up, installing, and troubleshooting Ethernet and IP based services. Y.1564 is the only standard test methodology that allows a complete validation of Ethernet service-level agreements (SLAs) in a single test.

For more information on the Y.1564. 10G internal mode, see the IP SLAs Configuration Guide, Cisco IOS XE Gibraltar 16.12.x (Cisco NCS 4200 Series).

New Hardware Features in Cisco IOS XE Gibraltar 16.12.1

There are no hardware features for this release.



CHAPTER 3

Caveats

This chapter describes open and resolved severity 1 and 2 caveats and select severity 3 caveats:

- The "Open Caveats" sections list open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.
- The "Resolved Caveats" sections list caveats resolved in a specific release, but open in previous releases.

The bug IDs are sorted alphanumerically.

Note The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat you must use the Bug Search Tool.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve effectiveness in network risk management and device troubleshooting. You can search for bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. For more details on the tool, see the help page located at http://www.cisco.com/web/applicat/cbsshelp/help.html

Open Caveats – Cisco IOS XE Gibraltar 16.12.8

There are no open caveats for this release.

Resolved Caveats – Cisco IOS XE Gibraltar 16.12.8

There are no resolved caveats for this release.

Open Caveats – Cisco IOS XE Gibraltar 16.12.7

There are no open caveats for this release.

Resolved Caveats – Cisco IOS XE Gibraltar 16.12.7

There are no resolved caveats for this release.

Open Caveats – Cisco IOS XE Gibraltar 16.12.6

Caveat ID Number	Description
CSCvo36974	Traffic drop is observed over IPSEC with dynamic modication in IPSEC tunnel and route
CSCvq93254	After IPV6 nd cache expired, transit traffic fails when ECMP enabled
CSCvs21550	The **snmpwalk** command is not retrieving vt description in mode vt-15.
CSCvs35755	CEM ACR: shut/no shut on physical SONET controller is causing path to go down
CSCvs82744	Shutting 1 BDI is affecting traffic on other tunnels
CSCvt57044	AINS to be disabled in VCOP and TPOP
CSCvu31005	Enable L-bit propogation in framed SATOP for LOF alarm
CSCvv58669	ROMMON region 0 and 1 verification CLI

Caveat ID Number	Description
CSCvw85788	BFD flaps due to ARP packet loss when other non priority classes congested
CSCvy81362	Controllers are down due to LP-LOP alarm After CE reboots
CSCvy91436	Egress QoS classification issues with Service instance 2 configuration on CE facing interfaces
CSCvz18784	Ingress QoS Policer not freed upon interface going down causing POLICERD leak

Resolved Caveats – Cisco IOS XE Gibraltar 16.12.6

Caveat ID Number	Description
CSCvv73547	Router crashed fib_loadinfo_max_oce_idx
CSCvv99456	ACL entries with FRAGMENT keywords are not working on the router
CSCvw93411	Interface counters not incrementing after 2 yrs, 22+ weeks on ASR920-24SZ-M variant
CSCvx24923	HS1 2.43 FPGA commit for reload/brom select issue
CSCvx41010	Failed to marshal xcvr_sync message: Bad address
CSCvx47340	When insert 10G XFP in 10 Gig port from 1Gig SFP, multicast traffic stops
CSCvx55831	Ingress policy with set qos-group action is creating extra TCAM entry with match on egress policy
CSCvx58983	Xconnect interface flapping when shut or no shut issued or hardware failure in path of Xconnect
CSCvx63370	With channelized T3 mode after IM OIR alarm clear or assert not happening for first T1.
CSCvx99501	Wrong snmp traps are generated for high voltage threshold violations
CSCvy16480	USB flashcards not mounted on new ASR-920-12CZ-A
CSCvy19318	MH-BFD over IPv6 stopped working after upgrade
CSCvy25392	Cannot delete recovered clock configuration from STS-3c

Open Caveats – Platform Independent Cisco IOS XE Gibraltar 16.12.6

Caveat ID Number	Description
CSCvy78284	Router crashes when zeroised RSA key is regenerated

Closed Caveats – Platform Independent Cisco IOS XE Gibraltar 16.12.6

Caveat ID Number	Description
CSCvx19209	ISIS crash is seen in isis_sr_tilfa_compute_protection
CSCvx26650	On configuring route tag under ISIS, TI-lFA does not form repair path
CSCvx37945	Crash happens when uea_mgr tries to write an error log
CSCvy20783	**show run all** does not list default value for debugging

Open Caveats – Cisco IOS XE Gibraltar 16.12.5

Caveat ID Number	Description
CSCvp12250	caam_jr and asfctrl error logs are observed with IPsec configuration on certain conditions
CSCvs47204	IPSEC - Kernel Crash observed on Reload with Traffic
CSCvs82744	Shutting 1 BDI is affecting traffic on other tunnels
CSCvt42842	Flood of SKB received from Kernel, and could not find SA kernel logs
CSCvu51238	Kernel log messages are seen on the console while doing config replace & interface flap
CSCvw86859	Router may not load-balance traffic on MPLS links even though having ECMP in RIB/CEF

Open Caveats – Platform Independent Cisco IOS XE Gibraltar 16.12.5

Caveat ID Number	Description
CSCvp98693	MLPPP IPV4 IW: Range for the mlppp group numbers does not match in the configuring CLI
CSCvr39157	Y1731 1DM receive is inactive after delete/add of SLA configuration
CSCvu77385	Full throughput not working priority shaper percent is greater ~40 over 100g nni
CSCvv74332	MAC not flushed/withdrawn in remote peer on VC swichover from active to standby
CSCvw06702	IP SLA Egress classification is not working.

Resolved Caveats – Cisco IOS XE Gibraltar 16.12.5

Caveat ID Number	Description
CSCvu95940	Egress QoS policy config missing on PoCh member link flap
CSCvu97978	Node crashed with core generation in 16.12 throttle
CSCvv16454	Traffic failure due to MPLS ECMP load-balancing in one of the labelled path
CSCvv24059	Mgr crash is noticed on RSP when EMPLSINTD is exhausted.
CSCvw34109	PTP failure due to LSMPI buffer exhaustion
CSCvr43362	NCS 4202: Fan speed control measures for overheating router

Resolved Caveats – Platform Independent Cisco IOS XE Gibraltar 16.12.5

Caveat ID Number	Description
CSCvu06475	Segment-routing cli cleanup under ospf failing after deleting segment-routing from global configuration
CSCvu23567	RSP3: BGP crash seen on Stand by router when 100 BGP sessions are established.
CSCvu44467	VRRP packets are generated with CS0 marking instead of CS6
CSCvv07825	SR uloop should only be calculated for best path
CSCvv42663	no snmp trap link-status under serial interface disappear after router reload
CSCvv79677	Router crashed after BGP flap

Open Caveats – Cisco IOS XE Gibraltar 16.12.4

Caveat ID Number	Description
CSCvq93254	After ipv6 nd cache expired, transit traffic fails when ECMP enabled
CSCvr07668	RSP2: FRR with Multi member POCH, LB not working
CSCvr68265	Write error: Bad address message seen with rommon upgrade command
CSCvs03683	Support for SFP Combo IM—8-port SFP Gigabit Ethernet + 1-port 10 Gigabit Ethernet
CSCvs53291	Backout of DDTS CSCvq93254
CSCvs96535	Dual rate port flaps during bootup - resulting VRRP issue
CSCvu14321	Router crashes at the moment of updating next hop
CSCvu49097	Ports on ASR920-12SZ-D are not coming up when 1G SFPs are used
CSCvu57353	SNMP: CPUHOG triggered by FPGA dying gasp
CSCvw34109	PTP failure due to LSMPI buffer exhaustion

Open Caveats – Platform Independent

Caveat ID Number	Description
CSCuu39858	Polaris_dev: VRF sub mode configurations under aaa group
CSCuw75352	ASR1k-lisp:Standby RP complains when eid-table removed from Active RP
CSCux68415	ASR1k: lisp instance are not operational with vrf Deletion error
CSCvh04941	Small bgp routing prefixes show as RIB-failure due to Mallocfail - subnet ndb with IWAN scale setup
CSCvo32390	show logging process does not decode files when number of new messages is low
CSCvo90459	Cisco-IOS-XE-native (isis): Redistribute application command have issues.
CSCvp60827	Delay of 30 sec while creating a new config file for phone using tftp.
CSCvq01379	Revert the changes of CSCvo75201 in rel21
CSCvq03975	ISIS multicast-intact issue with SR uloop EP.
CSCvq47186	L2 EVPN: Remote MAC not unfrozen when duplicate cleared with no MAC-only route
CSCvq84990	Remove show ip/ipv6 access-list from syncfd-<ewlc-SIT>17.1-Observed Traceback followed by IOSD crash

Caveat ID Number	Description
CSCvr09310	vManage should be able to work with cEdge banners in the same way as with vEdges
CSCvr09408	"tls" CLI is not working which is present under dspfarm profile
CSCvr24434	yang missing for "ipv6 locator reachability minimum-mask-length 128 proxy-etr-only"
CSCvr28935	IOS crash in DHCPd Receive with Unnumbered interfaces
CSCvr39428	L2 EVPN: no l2vpn evpn does not work correctly
CSCvr51558	Evpn import limit counter is wrong
CSCvr58056	Prefix SID and Manual Aj-SID range not correct
CSCvr80334	Pubd process on the controller goes down, managed by DNA-C 1.3.2
CSCvr83340	Add global "ip tcp mss" command to Cedge CLI and Yang
CSCvr91021	SESM Policy-Interface on ISG ignoring Radius Requests on port 1812
CSCvs02944	OSPFv3 distance command is missing per route-type distances for address-family ipv4
CSCvs13561	Post SSO, if service template is getting downloaded and switch crashes, client is stuck in authc
CSCvs15808	VRRPv3 failing on port-channel sub-interface.
CSCvs53280	TCP stuck in CLOSEWAIT when using X25 PVC RBP sessions on ISR 4k
CSCvs58945	Missing constraints and PRCs lead to broken model
CSCvs76180	IS-IS: SRMS Active Policy updates connected sids inappropriately
CSCvs93302	CDP Information Leakage Vulnerability
CSCvs98438	Inter vrf arp failing due to arp req filtered: it's our address
CSCvs99153	Not able to configure logging host <ipv4-addr> vrf <vrf-name>
CSCvt00228	DDNS triggers a crash when an update is sent to delete an entry
CSCvt03033	ISR4351:%BGP-3-BGP_SRTE_FAILURE: BGP SRTE failed to register with TE -Restarting BGP may be required
CSCvt12436	BGP SR ODN policy doesn't become UP.
CSCvt16988	Existing configuration on a cEdge could not be modified by a new template
CSCvt19590	Catalyst 9200L is not sending radius-server attribute 32
CSCvt51568	SR 688450700 : Switch member reloaded
CSCvt56647	TCP session is not established between catalyst 3850 and ISE servers
CSCvt58187	LISP Tracebacks seen on Border/CP node

Caveat ID Number	Description
CSCvt60188	Authentication Config Removal leads to Supervisor Crash
CSCvt65374	Local routes are getting leaked b/w vrf's along with Connected routes
CSCvt68348	Unexpected reload when using "show radius server-group all" or "show aaa server"
CSCvt73592	missing/corrupt IOS-XE PKSC10 format
CSCvt74331	C9300 console authorization does not fail back to local if radius server is not defined
CSCvt75633	It takes long until FlexVPN IKEv2 tunnel re-establishes when tunnel flaps
CSCvt94052	9800 WLC crashes when changing the password for existing user
CSCvt94212	%COMMON_FIB-SW1_DFC6-3-PATH_EXT_DUPLICATE after upgrade from 15-2(1)SY7 to 15.5(1)SY4
CSCvt99272	High CPU usage caused by "TCP Timer" process
CSCvu01690	CPUHOGS produced while executing the command - client fireall access-list ?
CSCvu06475	Segment-routing cli cleanup under ospf not happening after deleting segment-routing from Global
CSCvu06641	tacacs+ single connection packet flow
CSCvu12106	cedge: can not remove "ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr"
CSCvu16200	Router May Crash When a SSH session is Closed After a TACACS Configuration Change (Part 2)
CSCvu18265	Building Node Cache can consume high CPU when Segment Routing is not enabled
CSCvu27953	Crash due to a segmentation fault in the "IPsec background proc" process
CSCvu31813	ASR1k - valid Vendor Specific TLV dropped for invalid header length
CSCvu36475	Numbered ACLs fail to program to software TCAM if there's an object-group config
CSCvu36476	memory corruption in IOMEM in polaris 16.11.1
CSCvu40093	Crash when tearing down a PPPoE client session
CSCvu42109	Traceback: Standby RSP3 reloads "HSCF Failed to sync private-config"
CSCvu52322	CBR8: do not drop malformed dhcp option 125 packets
CSCvu55783	SSS Key (username) is not updated after receiving CoA with username
CSCvu58791	RADIUS not sent for 802.1x
CSCvu61753	3850 Not Starting MAB Process

Resolved Caveats – Cisco IOS XE Gibraltar 16.12.4

Caveat ID Number	Description
CSCvs36897	OCE consistency check on cEdge causes crash
CSCvt01082	IM deactivate CLI enabled for 10G IMs in Crete
CSCvt10032	ASR920_XE_BIT: CFM RMEP not getting learnt over VPLSoBkp PW BD
CSCvt21903	RSP2 Traffic drops observed with IPSec traffic
CSCvt32521	Duplex half change to full after reload
CSCvr43362	NCS 4202: Fan speed control measures for overheating router

Resolved Caveats – Platform Independent

Caveat ID Number	Description
CSCvs30865	rLFA for LDP causes loss of MPLS traffic after RSP switchover
CSCvs95815	C1111 telnet refused for link-local addresses when using ipv6 access class
CSCvt14323	ASR903 IGMP: reports received on mLACP Port-Channel dropped incorrectly
CSCvt25458	MPLS TE is not coming UP when bandwidth configured on Juniper head end

Open Caveats – Cisco IOS XE Gibraltar 16.12.3

Caveat ID Number	Description
CSCvt01082	IM deactivate CLI enabled for 10G IMs
CSCvw34109	PTP failure due to LSMPI buffer exhaustion

Open Caveats – Platform Independent

Caveat ID Number	Description
CSCvq76305	AutoRP listener functionality issue
CSCvs30865	rLFA for LDP causes loss of MPLS traffic after RSP switchover
CSCvs58498	High CPU on SNMP engine due to CISCO-CEF-MIB

Resolved Caveats – Cisco IOS XE Gibraltar 16.12.3

Caveat ID Number	Description
CSCvs74558	IPV6 Traffic causing Broadcast Storm on port with hwidx 3
CSCvr43362	NCS 4202: Fan speed control measures for overheating router

Resolved Caveats – Platform Independent

Caveat ID Number	Description
CSCvm79556	MSPW VC down after Switchover (Error Local access circuit is not ready for label advertise)

Open Caveats – Cisco IOS XE Gibraltar 16.12.2a

Caveat ID Number	Description
CSCvr26253	UDP and TCP traffic are not successful when through IPSec tunnel
CSCvr42356	IPSec: Changing IP addresses on LAN interface results in traffic failing over IPSec tunnel
CSCvr50508	Router_RP_0_fman_rp crash is observed on applying conditional crypto debug
CSCvr61371	BFD remains down when using PBR on BDI interface
CSCvw34109	PTP failure due to LSMPI buffer exhaustion

Open Caveats – Platform Independent

Caveat ID Number	Description
CSCux43298	**show interface pseudowire** command displays invalid peer information
CSCvn86673	Dialer watch does not disconnect the backup link even after the watched route exists in routing table
CSCvp60827	Delay of 30 sec is observed while creating a new configuration file for phone using TFTP
CSCvq50202	Class-attributes are duplicated after EAP reauthentication in ISG radius proxy scenario
CSCvq65438	Copying configuration file containing SmartPort macros to run fails
CSCvq69866	HSRPv2 crashes while retrieving group from received packet

Caveat ID Number	Description
CSCvq78692	mGRE L3VPN is broken after reload
CSCvq93089	Active switch crashes after standby is reloaded
CSCvq95479	Parser returns invalid PRC to certain commands
CSCvq96794	VPLS label misprogramming occurs after RSP switchover
CSCvr05504	Dialer interface counter does not correlate to the counter of interfaces bounded to
CSCvr08740	Router crashes after receiving EVPN route-type 2 without any ext-community
CSCvr08961	Switch stop responding to CoA
CSCvr18919	9400 SVL - Upon redundancy failover, route being purged on downstream device
CSCvr21440	3850 loops get-response value of object cafSessionClientMacAddress
CSCvr23104	BGP looped update is observed among 3 peers
CSCvr27393	Crash is observed on BGP Router process
CSCvr34118	Removes login and fix broken command
CSCvr34677	DHCP packets are not encrypted in redundant ip helper setup
CSCvr39868	Unexpected reload is observed when issuing **show ip mroute vrf <vrf> verbose** command
CSCvr45669	cEdge - Template is not pushed because of bad-command **no ip domain-name**
CSCvr49439	Multiple encapsulations of packet with L2TP headers crash ASR1K
CSCvr51079	PPPoE session is stuck in LCP state due to the wrong invoke of AAA method list
CSCvr54031	TBs are seen with scaled IP SLA configs with **ip sla reset** command
CSCvr57022	Routers are not removed from routing table when Dialer interface is shut
CSCvr57138	Wrong pointer to next buffer - Catalyst 9300
CSCvr57340	MAB is removed from template that causes authorization failure
CSCvr61879	**`static ip addresses not configured for the list`** message is observed
CSCvr70470	sessmgrd crashes with "clear dot1x mac" command
CSCvr73095	After AES encryption is enabled, entering plain aaa dynamic-author keys corrupts key
CSCvr74333	SMD memory leak is observed while sending radius packets
CSCvr74619	Cat 9000 switch crashes during Authentication Failure of Wired Client
CSCvr75640	LNS crashes with Segmentation fault (11) in L2TP mgmt daemon

Caveat ID Number	Description
CSCvr76555	IOS-XE 16.12.1a version, two redundant RPs, VPDN tunnel do not come up
CSCvr79052	cEdge 16.11.1a or 16.12.1b console 0 does not honor the privilege set in the username.

Resolved Caveats – Cisco IOS XE Gibraltar 16.12.2a

Caveat ID Number	Description
CSCvp86320	ASR920 CSDL : Hotspring1 secure FPGA
CSCvp86327	ASR920 CSDL: Hotspring2 secure FPGA
CSCvp86365	Cisco RSP2 Module CSDL : secure FPGA

Resolved Caveats – Platform Independent

Caveat ID Number	Description
CSCts28315	DHCP-pd reflects the Advertised prefix in Request message
CSCvi22263	Crash is observed when IOS adapts shaping with Adaptive QoS over DMVPN configured
CSCvj76866	Partial Power Failure in Stack Causes Interfaces to Become "shutdown"
CSCvm40566	IP prefix list replacement gets error from IOS side
CSCvo55194	After RSP switchover, label imposition is not programmed in Software on APS standby router
CSCvo55783	Pending objects are observed with respect to to uRPF on reload or soak script run
CSCvp38407	**radius-server attribute 31** command broken on LNS when LAC sends Remote-Id string
CSCvp66281	**default ip forward-protocol udp xx** command changes to **no ip forward-protocol udp xx** command after rollback
CSCvp74674	QoS fails to apply to tunnel2 when underlying tunnel1 reachability change
CSCvp96887	Fails to attach template to Cisco XE SDWAN Rtr if qos-map name is changed after policy-map is attached
CSCvq00263	Device crashes @ radius_io_stats_timer_handler due to dynamic-author
CSCvq04828	VRF aware reverse DNS lookup does not work
CSCvq04989	Ping between two interfaces does work; dialer interface is interfers in the ARP Processs

Caveat ID Number	Description
CSCvq09061	.py file check is unsuccessful while registering the policy and the error is seen
CSCvq18328	SSH: host_key->name is not null after reload which prevents SSH from starting up
CSCvq29953	IP SLA reacst for packet loss and successive packet loss does not set $_ipsla_react_type in EEM
CSCvq33004	Account logon fails for both direct and indirect lite-session in Cisco 16.9.3 Release
CSCvq34893	Template push to CEdge fails when you change the access VLAN on a switchport from VLAN 1
CSCvq35631	9300 crashes due to HTTP Core
CSCvq49721	Telnet access fails when VRF-aware extended VTY ACL is configured
CSCvq54265	IP bootp server is disabled by default as a device hardening best practice
CSCvq56114	Cat3k crashes in IGMP code due to invalid source count in DNS lookup
CSCvq56208	MDT: xpath union operator only outputs data from the left hand expression
CSCvq58265	BGP PIC Repair path breaks after link flap occurs
CSCvq58722	Python script register failure is observed when using custom directory instead of Flash
CSCvq59908	Stack crashes after upgrade
CSCvq60252	PBR works although an interface is down
CSCvq70148	BGP improperly formats the BGP ASSET attribute if ASSET attribute length is beyond 255
CSCvq72298	Router crashes on running **show policy-map interface <> output** command
CSCvq73364	mVPN - Multicast packets dropped and %MFIB-SW2-3-MFIB_CTXT_DEPTH_EXCEEDED is printed continuously
CSCvq89252	IP SLA for Path-Jitter returning a value which is not defined by the MIB
CSCvq94679	[SDA] Crash is observed due to Segmentation fault(11), Process = ARP Input
CSCvq95645	CAT9800 WLC crashes due to memory corruption
CSCvq97365	Two interfaces of client in different VRF connected to same vlan of server are not able to procure IP via DHCP
CSCvr00183	AAA accounting issue is observed after router reload occurs when mGRE and L3VPN are configured
CSCvr00344	**ip access-list logging hash-generation** commandremoves ACL statements upon reload
CSCvr02957	Re-add app-hosting move support is removed in version 16.12.1

Caveat ID Number	Description
CSCvr05406	LISP Map-cache is not updated correctly after wired Host-mobility
CSCvr09014	IGP metric is not detected in MPLS TE topology
CSCvr13213	Session is unauthorized as Redirect ACL Failure. Failed attribute name is POSTURE_REDIRECT.
CSCvr36887	9800 WLC crashes by WNCD process when modifying AAA configs from WebUI

-

Open Caveats – Cisco IOS XE Gibraltar 16.12.1

Caveat ID Number	Description
CSCvp59580	DR_10G_PORT_MAP is not correct during SFP OIR.
CSCvq00342	Duplicated packets on MVPN deployment on Cisco NCS router.
CSCvo36974	Data traffic drop is observed over VRF_AWARE_IPSEC with IPSEC profile removal and addition
CSCvp12219	IKEV1 tunnel goes down even after core port un-shut and comes up again
CSCvp28897	Kernel crash observed with 1500 frame size on core port shut or un-shut on peer
CSCvp61200	VRF AWARE IPSEC - One-way traffic hits tunnel during clear crypto process
CSCvp12250	The error logs such as caam_jr and asfctrl are observed
CSCvw34109	PTP failure due to LSMPI buffer exhaustion

Resolved Caveats – Cisco IOS XE Gibraltar 16.12.1

Caveat ID Number	Description
CSCvm50225	GRE: Unable to ping over GRE tunnel if packet size more than 1472 bytes
CSCvn49741	RSP2A-64 and RSP2A-128 _mgr crash.
CSCvn55871	T1 serial interface went down with encapsulation mode as PPP with remote loopback config as iboc.
CSCvo07619	BDI IPv6 ping failure_FMFP_OBJ_Download_Failure
CSCvo19770	Router crashes at hashtable_get_nth_entry
CSCvo35275	MVPN: Unable to pass high MTU multicast packets-MDT-MTU

Caveat ID Number	Description
CSCvo98627	The system stops responding due to nile_cef_adj_gre_delete when the router ospf shut is performed on peer
CSCvq10257	About incorrect I/F notation when enable qos-overhead-accounting Tengigabit interface
CSCvq01602	After IPv6 nd cache expired, transit traffic fails when ECMP