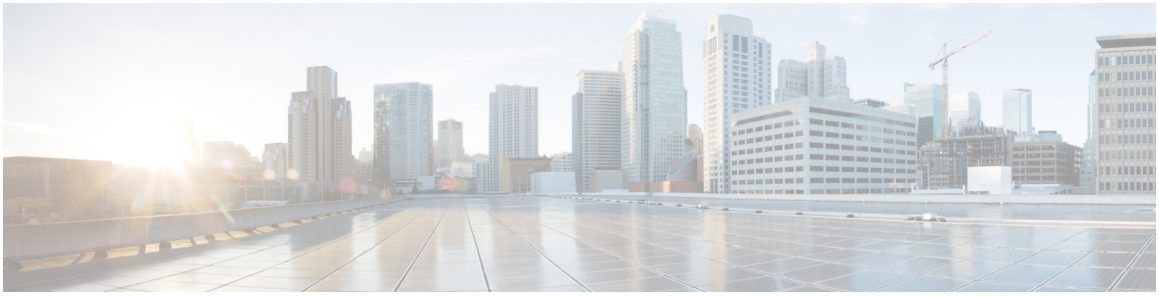
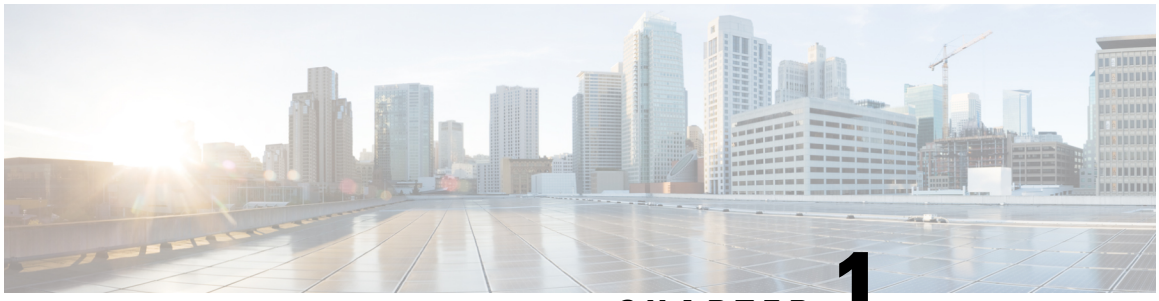
Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE Fuji 16.8.x

First Published: 2018-03-16

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.

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)

ROMMON Version

- NCS4201—15.6(31r)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 16.12.7 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 interface 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
  ```

- SSFPs are not supported.
- Virtual services should be deactivated and uninstalled before performing replace operations.
- For Cisco NCS 4202 Series:
  - 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.

Known Issues

Identifier	Description
CSCux22026	supress syslog messages while booting up for internal interfaces

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.

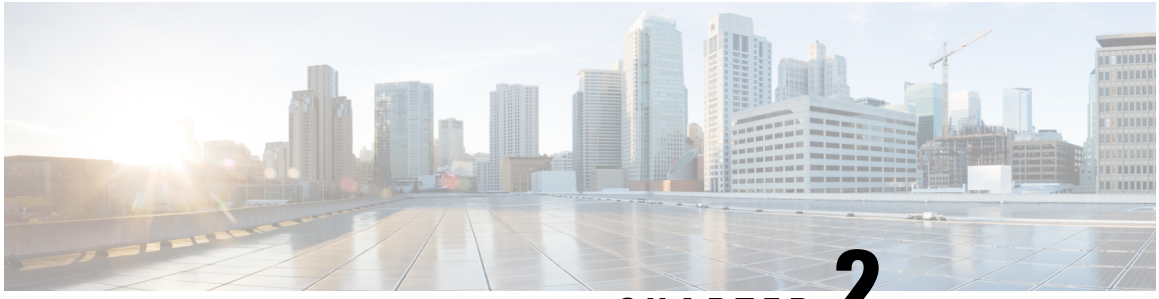
MIB Support

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 supported on the Cisco NCS 4200 Series in this release.

New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.8.1b

- **Egress QoS for IPSLA**

  The IPSLA packet classification is enabled in egress QoS. This feature enables you to apply classification and queueing on the egress interface for IPSLA packets. The egress interface can be either a Layer 2 interface under bridge domain interface (BDI) or a Layer 3 physical interface.

  The following new command is introduced for this feature:

  platform ipsla classify cpu packets

  For more information on Egress QoS for IPSLA, see the Quality of Service Configuration Guidelines, Cisco IOS XE 16.8.x (Cisco NCS 4200 Series).

  For more information on the new command, see the Cisco IOS Quality of Service Solutions Command Reference.

- **Programmability**

  - Model-Based AAA— Implements the NETCONF Access Control Model (NACM). NACM is a form of role-based access control (RBAC) specified in RFC 6536.
  - NETCONF Global Session Lock and Kill Session—Provides a global lock and the ability to kill non-responsive sessions in NETCONF. During a session conflict or client misuse of the global lock, NETCONF sessions can be monitored via the show netconf-yang sessions command, and non-responsive sessions can be cleared using the clear configuration lock command.
  - NETCONF and RESTCONF Debug commands—Commands for debugging were added.
  - NETCONF and RESTCONF IPv6 Support—Data model interfaces (DMIs) support the use of IPv6 protocol. DMI IPv6 support helps client applications to communicate with services that use IPv6 addresses. External facing interfaces will provide dual-stack support; both IPv4 and IPv6.

- YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1681

  Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same github location highlights changes that have been made in the release.

For more information on the Programmability features, see the Programmability Configuration Guide, Cisco IOS XE Fuji 16.8.x.

- **Support for Seven Level Priority Queues**

  The Cisco NCS now supports seven priority levels: level 1 (high) and level 7 (low). The device places traffic with a high-priority level on the outbound link ahead of traffic with a low-priority level. High-priority packets, therefore, are not delayed behind low-priority packets.

  For more information, see the QoS: Congestion Management Configuration Guide, Cisco IOS XE Release 3S (Cisco NCS 4200 Series).

- **VPLS over Backup Pseudowire**

  Pseudowire redundancy allows you to detect any failure in the network and reroute the Layer 2 service to another endpoint that can continue to provide service by providing additional backup pseudowire. This feature provides the ability to recover from a failure of either the remote provider edge (PE) router or the link between the PE and customer edge (CE) routers.

  For more information, see the MPLS Layer 2 VPNs Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series).

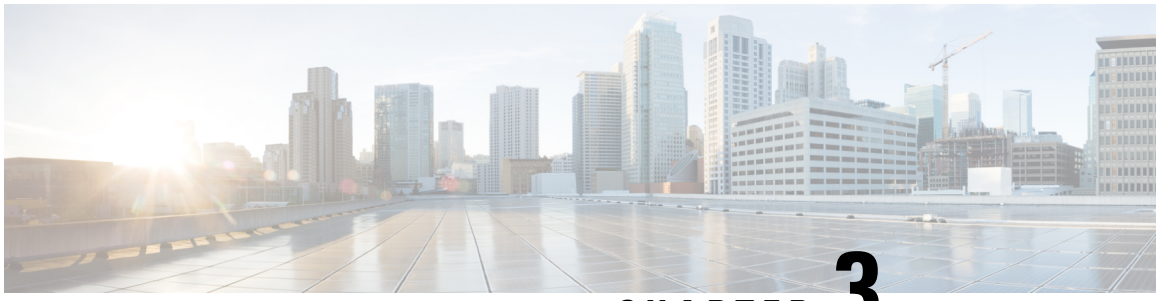
- **Latching Loopback**

  Latching loopback feature is supported.

  For more information, see the Carrier Ethernet Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series).

New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.8.1b

There are no new hardware features in 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 Fuji 16.8.1b

Caveat ID Number	Description
CSCvd58258	IOS-XE display issue show hw-module subslot X/X transceiver X idprom detail
CSCvf96598	RSP2 : ~15sec loss traffic for /HSPW service on ISSU/sso
CSCvg01047	G275.2 disqualified the dynamic port even before it completely negotiated the session

Caveat ID Number	Description
CSCvg08374	Trace back logs are seen on Striker while loading polaris baseline image
CSCvg23724	QOS fails to secure teleprotection traffic on MLPPP interface
CSCvg84664	Port does not come up with hard loopback inserted
CSCvh05198	Class-map association to policy-map dynamically throws debug errors on logging
CSCvh55399	T1 Service Latency is Asymmetric in a Simple Linear Topology
CSCvh77376	Chassis Fails to drop to rommon after a crash
CSCvh88811	RSP2 GRE:PIM neighbor ship fails to come up on VRF instance when outgoing interface is BDI
CSCvi04483	EOMPLS traffic drop - Imposition FID and Disposition label is set to "NULL"
CSCvi06424	Traffic fails after moving/relearning mac-address from EFP to Xconnect interface
CSCvi10095	UDLD Err Disable (Admin down) observed on performing reload operations
CSCvi12362	convergence coming high on doing local_shut on Pegasus
CSCvi18644	BFD flaps during SSO
CSCvi25777	VID-84-Several Parameter Counters in "sh interfaces gigabitEthernet x/x/x" do not function in 4202

Resolved Caveats – Cisco IOS XE Fuji 16.8.1b

Caveat ID Number	Description
CSCvc27630	Tx Packets or Tx Bytes generated is always lesser than configured rate-steps
CSCvd75495	Wrong marking for locally generated packet of BFD,LDP, and BGP
CSCvd87285	Display issue - Egress i/f and L2 stats shows "unknown" and no packet drops
CSCve05859	Exxx EIN: G.8275.1 testing: Clock loop forming between synce and ptp
CSCvf10783	Arbitrary File Overwrite Vulnerability
CSCvf49124	Management default gateway not reachable with 16.6.1 image
CSCvf55327	CLNS interop with ONS not working
CSCvf60263	APS-ACR Scale Issue:For 8K Scale Config, PW-GROUP not bound on Arrive CEM FPGA during Copy Config
CSCvf68605	DHCP Snooping Database restore/renew failing on all variants

Caveat ID Number	Description
CSCvf69983	Packets not looped back 100% for LLF-external when Responder present in MIP
CSCvf80056	MAC-FLAP-Syslog-Not generated for TEFP BDs
CSCvf80724	Complete traffic drop (imp and disp) over VPLS Act PW
CSCvf96793	DS3 VCOP AIS raised for J1 byte mismatch
CSCvf99074	Ping Loss on Built-in Te 0/0/10 or 0/0/11 Port and CRC / MAC Errors at Peer End
CSCvg04717	DDR Busy and Calibration handling in FPGA software driver
CSCvg14825	Require varbind entSensorPrecision,Scale & Type along with trap entSensorThresholdNotification
CSCvg21893	Unexpected traffic was sent out from router access port from REP ring
CSCvg21899	Traffic forwarding not happening for VLANs added via "encap dot1q add" command in TEFP
CSCvg23956	VPLS Backup PW: Enable member bdi CLI under l2vpn xconnect context
CSCvg26930	Ten Gig interface going into admin down state after one gig shut down
CSCvg31959	MLPQ does not work on dynamic modification of queue-limit in higher priority level class.
CSCvg36200	IPv4 deny ACL applied in the BDI is blocking L2 switched traffic under certain conditions
CSCvg44405	WRT : storm-control unable to fetch correct level in percentage value, hence failing to take action
CSCvg53877	Egress QOS Fails when speed is changed at interface via nego auto, speed cli command
CSCvg63915	2 Xconnect TDL Messages Leaked in Cylon_Mgr on "show running-config"
CSCvg70409	IOT: For Serial IM, flowcontrol is not applicable
CSCvg79798	"ZTP reset" as last reload reason in IOS when ZTP button pressed > 8sec
CSCvg83081	Fixed Ports moving to admin down state after IMA8S insertion
CSCvg85163	ZTP not triggered with Gratuitous ARP
CSCvg88049	Remove IOS syslog message for link status IDLE
CSCvg93982	IOS XE entSensorThresholdNotification trap is not generated for Card Temperature
CSCvh03346	Fan speed display in IOS not matching the actual written value and read value
CSCvh06736	Device crashes on dynamically attaching a class to a policy .
CSCvh20282	Traffic is not flooding on all the interface for same TEFP BD

Caveat ID Number	Description
CSCvh51154	Dest-mac + type-field in Ethernet header checks need to be added for G-arp packets to trigger ZTP
CSCvh68935	BFD Flap on the link between RSP3 (8x10G) and RSP2 (Combo 10G) with switchover
CSCvh83722	All BFD Sessions Down as FPGA Stuck due to invalid Packet Length and Offset Error in DDR3
CSCvi06424	Traffic fails after moving/relearning mac-address from EFP to Xconnect interface