Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE Bengaluru 17.5.x

First Published: 2021-03-31

Last Modified: 2023-03-02

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Introduction** 1

Documentation Updates 1

Cisco NCS 4201 and Cisco NCS 4202 Overview 2

Feature Navigator 2

Hardware Supported 2

Determining the Software Version 3

Bundled FPGA Versions 3

Limitations and Restrictions on the Cisco NCS 4201 and Cisco NCS 4202 Series 4

Additional References 5

CHAPTER 2 **What's New in Cisco IOS XE Bengaluru 17.5.x** 7

What's New in Hardware for Cisco IOS XE Bengaluru 17.5.x 7

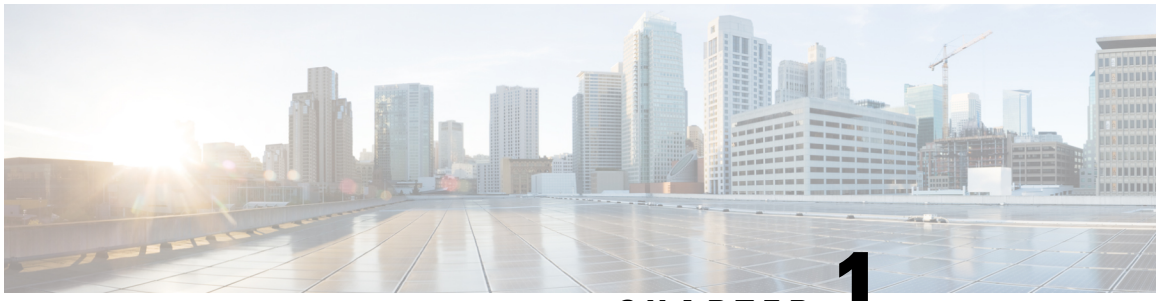
What's New in Software for Cisco IOS XE Bengaluru 17.5.x 7

CHAPTER 3 **Caveats** 11

Resolved Caveats – Cisco IOS XE Bengaluru 17.5.1 11

Open Caveats – Cisco IOS XE Bengaluru 17.5.1 12

Cisco Bug Search Tool 12



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, on page 1
- Cisco NCS 4201 and Cisco NCS 4202 Overview, on page 2
- Feature Navigator, on page 2
- Hardware Supported, on page 2
- Determining the Software Version, on page 3
- Bundled FPGA Versions, on page 3
- Limitations and Restrictions on the Cisco NCS 4201 and Cisco NCS 4202 Series, on page 4

Documentation Updates

Rearrangement in the Configuration Guides

- The following are the modifications in the CEM guides.
  - Introduction of the Alarm Configuring and Monitoring Guide:

    This guide provides the following information:
    - Alarms supported for SONET and SDH, and their maintenance
    - Alarm profiling feature

- Auto In-Service States for cards, ports, and transceivers

For more information, see the Alarm Configuring and Monitoring Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series).

- Rearrangement of Chapter and Topics in the Alarm Configuring and Monitoring Guide:
  - The Auto In-Service States Guide is now a chapter inside the Alarms Configuring and Monitoring Guide.
  - Alarms at SONET Layers topic in the following CEM guides, is added to the Alarms Configuring and Monitoring Guide:
    - 1-Port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module Configuration Guide
  - The Alarm History and Alarm Profiling chapters are removed from the below CEM Technology guides, and added into the Alarm Configuring and Monitoring Guide:
    - 1-Port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module Configuration Guide

- Configuring IEEE 802.3ad Link Bundling is now available in Ethernet Channel Configuration Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series).

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(44r)S
- NCS4202—15.6(43r)S

Bundled FPGA Versions

The following are HoFPGA versions bundled in the IOS:

- NCS4201—0X00030015
- NCS4202
  - BFD—0X0003001B
  - Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—0x10050071

The following are HoFPGA versions bundled in the IOS for 17.5.1 release:

- NCS4201—0X00040019
- NCS4202
  - BFD—0X0003001e
  - Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—NA

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

Note The error message "PLATFORM-1-NOSPACE: SD bootflash : no space alarm assert" may occur in the following scenarios:

- Any sector of SD Card gets corrupted
- Improper shut down of router
- power outage.

This issue is observed on platforms which use EXT2 file systems.

We recommend performing a reload of the router. As a result, above alarm will not be seen during the next reload due to FSCK(file systems check) execution.

However, If the error persists after a router reload, we recommend to format the bootflash or FSCK manually from IOS.

- 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, Cisco IOS XE 17.
  - 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.
- One Ternary Content-Addressable Memory (TCAM) entry is utilized for Segment Routing Performance Measurement. This is required for the hardware timestamping to function.
- Before installing the Cisco IOS XE Amsterdam 17.3.1, you *must* upgrade the ROMMON to version 15_6_43r_s or higher to avoid bootup failure. This is applicable to Cisco NCS 4202 routers. This workaround is not applicable to devices installed with ROMMON version 15.6(9r)S.

- While performing an auto upgrade of ROMMON, only primary partition is upgraded. Use the **upgrade rom-mon filename** command to upgrade the secondary partition of the ROMMON. However, the router can be reloaded during the next planned reload to complete the secondary ROMMON upgrade.
- For Cisco IOS XE Amsterdam 17.3.x , a minimum diskspace of 2 MB is required in the boot flash memory file system for a successful ROMMON auto upgrade process. For a diskspace lesser than 2 MB, ROMMON auto upgrade fails and the router reboots.
- Some router models are not fully compliant with all IETF guidelines as exemplified by running the pyang tool with the lintflag. The errors and warnings exhibited by running the pyang tool with the lint flag are currently non-critical as they do not impact the semantic of the models or prevent the models from being used as part of the toolchains. A script is provided, **check-models.sh**, which runs pyang with lint validation enabled, but ignoring certain errors. This allows the developer to determine what issues may be present.

  As part of the model validation for this Cisco IOS XE Amsterdam 17.3.1 release, "LEAFREF_IDENTIFIER_NOT_FOUND" and "STRICT_XPATH_FUNCTIONS" error types are ignored.
- Starting with Cisco IOS XE Bengaluru Release 17.5.1, if IPv6 Global IP is configured as the BFD peer, and if the interface goes down, a VRRP flap may occur. This may occur because, VRRP works on the basis of Link-local IP and not global IP. As a result, VRRP flaps on the previously backed up device and prints a DAD message.

Additional References

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.

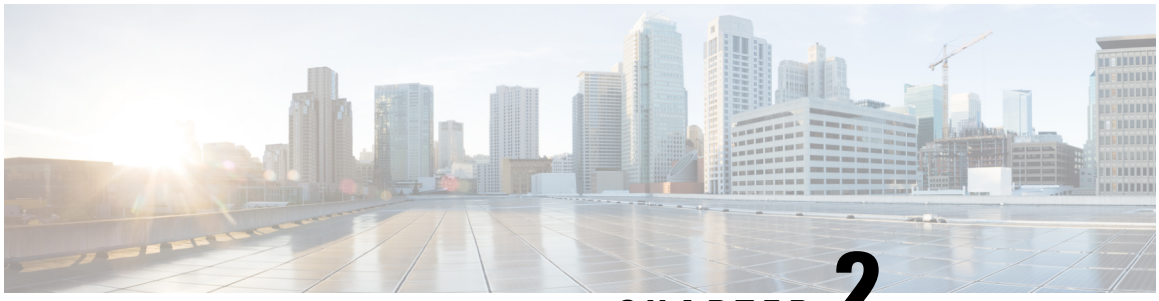
MIB Support

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

What's New in Cisco IOS XE Bengaluru 17.5.x

This chapter describes the new hardware and software features supported on the Cisco ASR 920 Series routers in Cisco IOS XE Bengaluru 17.5.x.

For information on features supported for each release, see Feature Compatibility Matrix.

- What's New in Hardware for Cisco IOS XE Bengaluru 17.5.x, on page 7
- What's New in Software for Cisco IOS XE Bengaluru 17.5.x, on page 7

What's New in Hardware for Cisco IOS XE Bengaluru 17.5.x

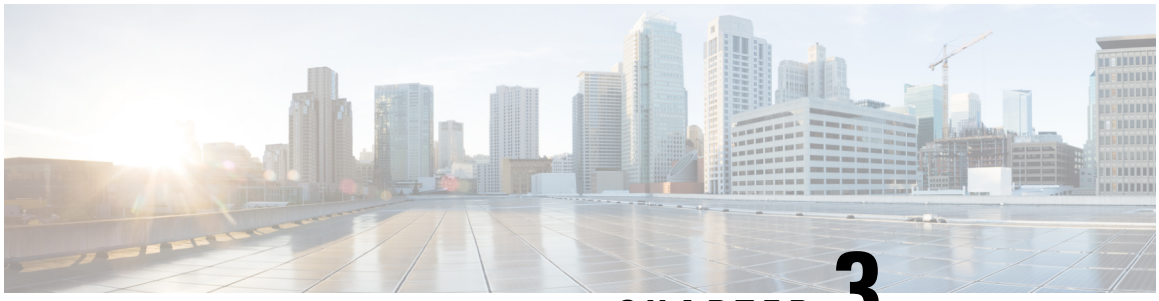
There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.5.x

Feature	Description
1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module	
Unframed Framing Support on E1 and Channel STM links	In this release, a new framing mode unframed is supported for the 1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module. With the unframed mode, you can create serial interface under the SDH VC12 mode.
Carrier Ethernet	
CFM Sessions Hardware Offload	This feature enables for effective CPU utilization by offloading the one second CCM interval sessions on the hardware.
Cisco NCS 4200 Series Software	
SNMP Dying Gasp Enhancement	This feature enables FPGA based effective space utilization between Ethernet OAM and SNMP. Use the **platform-oam-snmp-dg-enable** command on Cisco router to configure this feature.
High Availability	

Feature	Description
Secondary ROMMON Version Auto Upgrade	After primary ROMMON version is auto upgraded, secondary ROMMON version auto upgrade process takes place. The secondary ROMMON upgrade is only completed during the next planned manual reload of the router. This is applicable to NCS 4201/4202 routers.
IP SLAs	
TWAMP Light	This feature enables you to configure a TWAMP Light session using the **ip sla responder twamp-light test-session** command.
MPLS Layer 2 VPNs	
EVPN Integrated Routing and Bridging (L2 and L3 Anycast Gateway) and Data Center Interconnect or Border Leaf (Single Homing)	This feature allows the devices to forward both layer 2 or bridged and layer 3 or routed traffic providing optimum unicast and multicast forwarding for both intra-subnets and inter-subnets within and across data centers. Data Center Interconnects (DCI) products are targeted at the Edge or Border Leaf (BL) of data center environments, joining data centers to each other in a point-to-point or point-to-multipoint fashion, or at times extending the connectivity to internet gateways or peering points. This feature is supported on Cisco NCS 4201/4202 routers.
On-Change Notifications for L2VPN Pseudowire	This feature allows you to subscribe on-change Network Configuration Protocol (NETCONF) notifications for L2VPN pseudowire. You can generate an alert from a device when the pseudowire status changes.
QoS: Policing and Shaping	
IP Address Range-Based Filtering Support for CoPP ACL - RSP2	The CoPP ACL feature supports Ingress on In-band Management Loopback interface and Ingress on Data plane interface to block traffic using MPLS. CoPP ACL also enables you to configure the 830 and 5432 ports on the Cisco router. Source IP/Destination IP based filtering are also supported.
Segment Routing	
SR-PM Delay Deduction (Loopback Mode)	This feature improves the SR-PM detection time as the PM probes are not punted on the remote nodes. Also, it does not a require a third-party support for interoperability.
SR-TE PM: Liveness of SR Policy Endpoint	This feature enables Performance Measurement (PM) liveness detection and delay measurement for an SR policy on all the segment lists of every candidate path that are present in the forwarding table using PM probes. Thus, you can easily monitor the traffic path and efficiently detect any drop of traffic due to cable or hardware or configuration failures.This feature provides the following benefits: • End-to-end liveness is verified before activating the candidate path in the forwarding table. • End-to-end liveness failure can trigger re-optimization to another path by deactivating the current path.

Feature	Description
Segment Routing Flexible Algorithm with OSPF	This feature allows you to configure Segment Routing Flexible Algorithm with OSPF. Flexible Algorithm with OSPF supports metric minimization and avoidance, multi-plane, delay metric with rounding, and ODN with auto-steering.
Segment Routing Policy Counters	This feature enables statistic counters to be displayed when traffic passes over the SR-TE tunnel. You can use the command **show segment-routing traffic-eng policy name** *policy name* to view the counters.



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.

- Resolved Caveats – Cisco IOS XE Bengaluru 17.5.1, on page 11
- Open Caveats – Cisco IOS XE Bengaluru 17.5.1, on page 12
- Cisco Bug Search Tool, on page 12

Resolved Caveats – Cisco IOS XE Bengaluru 17.5.1

Caveat ID Number	Description
CSCvs50029	Interface flaps and input errors seen with optics GLC-FE-100BX-D in the router
CSCvv21542	Command to change from dynamic to static FAN algorithm for the router
CSCvv23077	config failure is seeen from 16_9_4 to 17_3_1 images upgrade
CSCvv42595	REP flapping randomly and frequently due to port down
CSCvv72192	IMA2Z IM, XFP and SFP+ are present and then XFP is removed LED still shows as green
CSCvv99456	ACL entries with FRAGMENT keywords are not working on the router
CSCvw64784	RSP2 CEM ACR: Not able to reuse same clock id on another controller After deleted clock id.

Caveat ID Number	Description
CSCvw93411	Interface counters are not incrementing after 2yrs, 22+ weeks on the router
CSCvx24923	FPGA commit for reload or brom select issue
CSCvr43362	NCS 4202: Fan speed control measures for overheating router

Open Caveats – Cisco IOS XE Bengaluru 17.5.1

Caveat ID Number	Description
CSCvw38827	Observing RSP2A-64 and RSP2A-128 logs in Cisco RSP2 HA router with CEM
CSCvx42526	A900-IMA2Z IM is impacted during SSO

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