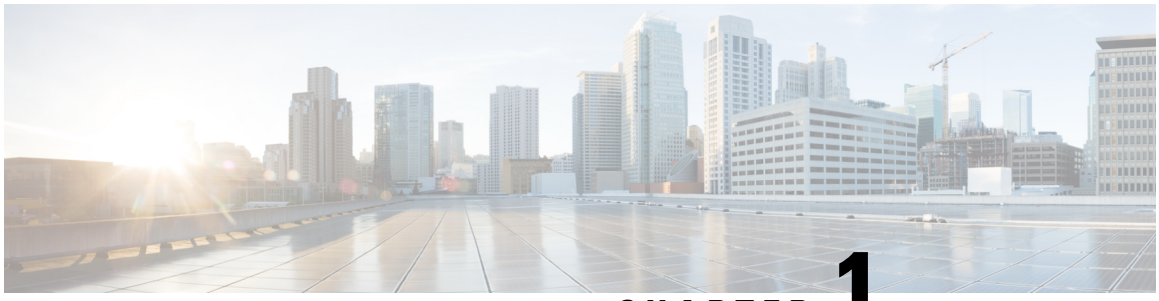
Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE Bengaluru 17.4.x

First Published: 2020-11-30

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

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 17.4.2 release:

- NCS4201—0X00030016
- NCS4202—0X0003001e

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, secondary ROMMON partition is also auto upgraded after a successful primary ROMMON partition upgrade is complete. You can reload the router at the next planned reload to complete the secondary ROMMON upgrade.
- For Cisco IOS XE Amsterdam Release 17.3.x, Cisco IOS XE Bengaluru Release 17.4.x, and earlier, the secondary ROMMON partition is not auto upgraded. You must manually upgrade it using the **upgrade rom-mon filename** command.
- Starting with ROMMON release version 15.6(43r)S, ROMMON version is secure. Once the ROMMON version is upgraded, it cannot be downgraded to a non-secure ROMMON version.
- Secure ROMMON is supported from Cisco IOS XE Amsterdam Release 17.3.1 onwards. However, it is compatible with all the releases.

  Any future secure ROMMON upgrade or downgrade is only possible from Cisco IOS XE Amsterdam Release 17.3.1 onwards.
- Any non-secure FPGA bundled releases moving to Cisco IOS XE Bengaluru Release 17.3.x or future releases can result in an FPGA upgrade and a ROMMON upgrade. If FPGA upgrade happens parallely with the ROMMON upgrade, you can only expect a single reload. If FPGA upgrade gets delayed and happens post ROMMON upgrade, two reloads are expected to complete both the upgrade processes. This is followed by a successful bootup of the target release image.

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.

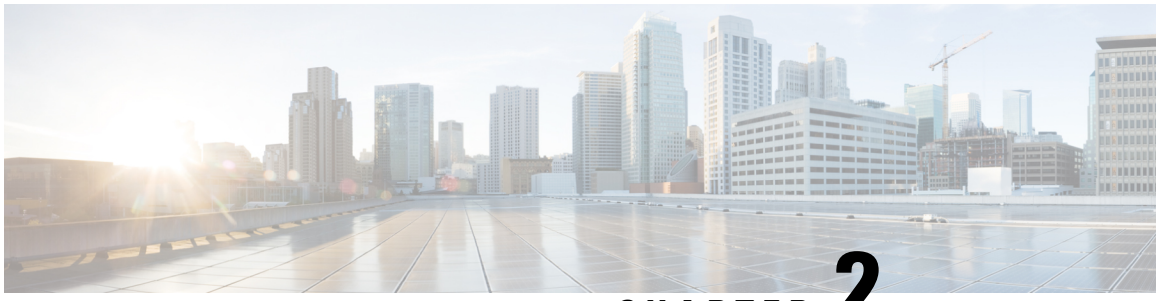
MIB Support

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 for Cisco IOS XE Bengaluru 17.4.x

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

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

What's New in Hardware for Cisco IOS XE Bengaluru 17.4.2

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.4.2

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.4.x

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.4.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	
IPv6 VLAN Handoff and 4k iMSG scale	VLAN handoff supports IPv4 and IPv6 local connect and cross connect.

Feature	Description
STS1E Framed SAToP Support on IMA3G	Support on clock recovery on STS-1e controller for framed SAToP on the following modes: • T3 • CT3 • VT-15
Carrier Ethernet	
Enabling the Bridge Domain Interface	This feature allows you to configure the **platform bdi enable-state up** global command.
IP Routing: BFD	
BFD over G8032 and Multi EFP BDI	Scale numbers for BFD and hardware offload are enhanced for the ASR 900 Cisco RSP2 module.
IP Multicast: Multicast	
Multicast SLA Measurment with MLDP	Display of aggregated egress multicast stats for BDI interfaces on Head node, which is part of the MLDP core is supported.
IP SLAs	
Configurable User-Defined and EMIX Packet Size	This feature allows you to configure user-defined and Enterprise traffic (EMIX) packet sizes. Use the following commands to configure user-defined and EMIX packet sizes: • **packet-size user-defined** *packet size* • **packet-size emix sequence** *emix-sequence* [**u-value** *u-value value*]
EMIX Sequence Enhancement	This feature enables SAT based support for configurable EMIX traffic pattern in FPGA-based SAT.
Layer 2	
Enhanced Ethernet Data Plane Loopback	The Ethernet data plane loopback feature is enhanced to avoid control packets getting dropped. The enhancement supports internal shaper configuration, when terminal ELB session is activated or deactivated to rate the limit the ELB session traffic. The enhancement is applicable only on internal loopback.
MPLS Basic	

Feature	Description
Re-optimization with Tunnel Bandwidth Modification on Flex-LSP Protect Path	This feature supports Make Before Break (MBB) functionality and thus ensures there is no traffic loss when a MPLS Flex LSP tunnel runs on protect LSP (if working LSP goes down) and the tunnel bandwidth is modified. When the working LSP comes up, use the following command to manually switch from the working to protect LSP: **mpls traffic-eng switch tunnel** *tunnel-ID*
Segment Routing	
L2VPN over SR-TE Preferred Path	This feature allows you to configure an SR policy as the preferred path for a VPWS or VPLS pseudowire. VPWS or VPLS pseudowires between same PEs can be routed over different SR policies based on the requirements. Prior to this release, you could only steer the traffic using the SR policy for routing IPv4 traffic to a destination pseudowire (over IGP or BGP-LU).
PCE Initiated SR Policy with OSPF Autoroute Announce	This feature enables a steering mechanism in which IGPs automatically use the policy for destination's downstream of the policy end point.
Segment Routing Flexible Algorithm support for TI-LFA uLoop Avoidance, SID Leaking, and ODN with Auto-Steering	This feature allows you to compute Loop Free Alternate (LFA) paths, TI-LFA backup paths, and Microloop Avoidance paths for a particular Flexible Algorithm using the same constraints as the calculation of the primary paths for such Flexible Algorithms, for IS-IS. See Calculation of Flexible Algorithm Path. Inter-area leaking of Flexible Algorithm SIDs and prefixes and selectively filtering the paths that are installed to the MFI are also supported. See Flexible Algorithm Prefix-SID Advertisement and Installation of Forwarding Entries for Flexible Algorithm Paths.
Telemetry (Model-Based Telemetry and Event-Based Telemetry) Support for Performance Measurement	This feature enables Model-Based Telemetry (MDT) and Event-Based Telemetry (EDT) that allow the data to be directed to a configured receiver. This data can be used for analysis and troubleshooting purposes to maintain the health of the network. The **sr_5_label_push_enable** SDM template is mandatory for this feature to function.

Other Supported Features

- Complete YANG Model for Ethernet EVC Configuration – An Ethernet Virtual Connection (EVC) is defined by the Metro-Ethernet Forum (MEF) as an association between two or more user network interfaces that identifies a point-to-point or multipoint-to-multipoint path within the service provider network. An EVC is a conceptual service pipe within the service provider network.

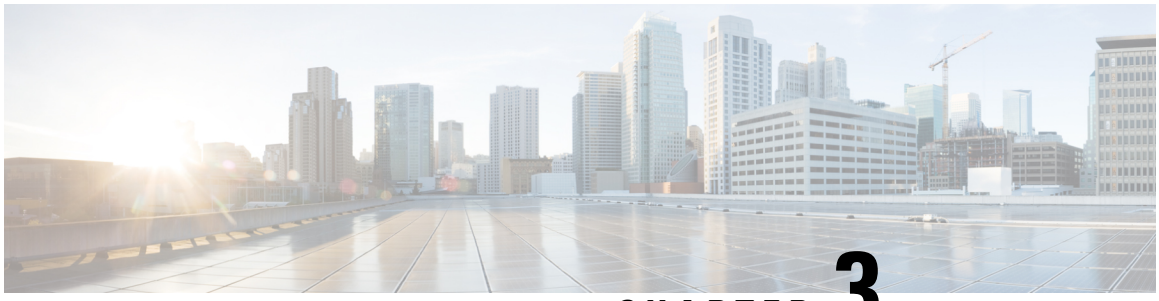
  YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1741.

  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.

- Complete YANG Model for CFM Configuration – Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service-instance Ethernet layer operations, administration, and maintenance (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

  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/1741.

  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.



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 17.4.2

Caveat ID Number	Description
CSCvu99207	Router: Incorrect STP forwarding state programming in platform.
CSCvw82303	Support for multicast route leaking in native multicast
CSCvw85511	BDI interface is causing high cpu usage.
CSCvw93411	Interface counters not incrementing after 2yrs, 22+ weeks on Router
CSCvx01642	PPPoE tag circuit-id remote-id should not be trusted if the interface is in untrusted mode
CSCvx24923	HS1 2.43 FPGA commit for reload/brom select issue

Caveat ID Number	Description
CSCvx41010	Failed to marshal xcvr_sync message: Bad address
CSCvx55831	Ingress Policy with set qos-group action is creating extra TCAM entry with match on Egress Policy
CSCvx99501	Wrong snmp traps are generated for high voltage threshold violations
CSCvr43362	NCS 4202: Fan speed control measures for overheating router

Resolved Caveats – Cisco IOS XE Bengaluru 17.4.2 - Platform Independent

Caveat ID Number	Description
CSCvv79677	Router crashed after BGP flaps
CSCvx19209	ISIS crash in isis_sr_tilfa_compute_protection
CSCvx26650	On configuring route tag under ISIS, TI-lFA is not forming repair path

Open Caveats – Cisco IOS XE Bengaluru 17.4.2

There are no Open caveats for this release.

Resolved Caveats – Cisco IOS XE Bengaluru 17.4.1

Caveat ID Number	Description
CSCvk22965	Bulk License "Out of Compliance" support
CSCvs34482	ISSU is not working on Cisco ASR 900 RSP2 nodes
CSCvt33153	Traceback is seen with the following message: `mroute_stats_update`
CSCvt69921	RSP2-128: CMAND core during SSO
CSCvt75327	v1731: Traffic is not seen after performing SSO in Imsg_Mix mode
CSCvt76777	Adj err obj is seen on removing sr-label-preferred
CSCvt78211	A900-IMA3G-IMSG:Serial interface gets blocked after reaching count of 700 for non acr and non pg
CSCvt92428	RSP2-128: Step by Step ISSU CMD is not working

Caveat ID Number	Description
CSCvt93010	Traffic drop is seen after Kernel log messages are seen while shut or no shut on Phy/BDI interfaces
CSCvu06547	Require varbind entSensorseveriry along with trap entSensorThresholdNotification
CSCvu13886	v174: Card protection performs shut or no shut on the CPG STS-1e, SLOS alarm is observed on the peer device
CSCvu29991	Historic performance intervals are not present for STS-1e interfaces in the command and SNMP MIB
CSCvu38550	For VCOP configured with type DS3, applique type should be Subrate T3 instead of Channelized T3/T1
CSCvu45472	1-port OC48 1/ STM-16 or 4-port OC-12/OC-3 / STM-1/STM-4 + 12-Port T1/E1 + 4-Port T3/E3 CEM Interface Module:Serial interface gets blocked after reaching count of 700 for acr and pg
CSCvu45833	ISSU: 1612-173: CEM Ckt is stuck at Setup Failed
CSCvu51472	Support for SAToP payload 64 byte and dejitter 2 ms in LOTR IMs
CSCvu59602	17.3.1-with transform-set esp-aes complete traffic drop seen after doing clear crypto session
CSCvu66126	OC-192 APS group is stuck with signal Fail condition
CSCvu78801	PPPoE VSA tags get overwritten at each PPPoE IA
CSCvu83291	Cylon_mgr memory leak is observed due to QoS policer
CSCvu89908	Crash is observed while doing clear crypto session soak run
CSCvu95940	Egress QoS policy configuration is missing on PoCh member link flap
CSCvu92363	SSD: harddisk is full but received %PLATFORM-1-NOSPACE: bootflash : no space alarm assert
CSCvu97954	MAC flaps are observed when using VPLS over backup pseudowire configuration
CSCvu97978	XE BIT : Cisco ASR 900 RSP2 node is crashed with core generation in 16.12 throttle
CSCvv16454	Traffic failure occurs due to MPLS ECMP load-balancing in one of the labelled path
CSCvv24059	RSP2-128 mgr crash is noticed on Cisco ASR 900 RSP when EMPLSINTD is exhausted
CSCvv31617	e2e circuit does not ping, serial interface is up and line protocol is up
CSCvr43362	NCS 4202: Fan speed control measures for overheating router

Open Caveats – Cisco IOS XE Bengaluru 17.4.1

Caveat ID Number	Description
CSCvv87440	Clock class 6 is advertised immediately on T-GM connection restore
CSCvv72192	When IMA2Z IM, XFP and SFP+ are present and then XFP is removed, LED still shows as green
CSCvw34109	PTP RX failure is observed due to LSMPI buffer exhaustion

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