



Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE 17.13.x

First Published: 2023-11-23

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 1

- Cisco NCS 4201 and Cisco NCS 4202 Overview 1
- Feature Navigator 2
- Hardware Supported 2
- Determining the Software Version 2
- Upgrading to a New Software Release 2
- Bundled FPGA Versions 3
- Limitations and Restrictions on the Cisco NCS 4201 and Cisco NCS 4202 Series 3

CHAPTER 2

What's New for Cisco IOS XE 17.13.x 5

- What's New in Hardware for Cisco IOS XE 17.13.1 5
- What's New in Software for Cisco IOS XE 17.13.1 5

CHAPTER 3

Caveats 7

- Resolved Caveats – Cisco IOS XE 17.13.1 7
- Open Caveats – Cisco IOS XE 17.13.1 8
- Cisco Bug Search Tool 8



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](#), on page 1
- [Feature Navigator](#), on page 2
- [Hardware Supported](#), on page 2
- [Determining the Software Version](#), on page 2
- [Upgrading to a New Software Release](#), on page 2
- [Bundled FPGA Versions](#), on page 3
- [Limitations and Restrictions on the Cisco NCS 4201 and Cisco NCS 4202 Series](#), on page 3

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(56r)S
- NCS4202—15.6(54r)S

Upgrading to a New Software Release

Only the latest consolidated packages can be downloaded from Cisco.com; users who want to run the router using individual subpackages must first download the image from Cisco.com and extract the individual subpackages from the consolidated package.

For information about upgrading to a new software release, see the [Upgrading the Software on the Cisco NCS 4200 Series Routers](#).

Upgrading the FPD Firmware

FPD Firmware packages are bundled with the software package. FPD upgrade is automatically performed on the router.

If you like to manually change the FPD Firmware software, use the **upgrade hw-module subslot 0/0 fpd bundle** to perform FPD firmware upgrade.

Bundled FPGA Versions

The following are HoFPGA versions bundled in the IOS for 17.13.1 release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202
 - BFD—0X00040009
 - Netflow—0X00040009

The following is the CEM FPGA version:

- NCS4202—0X00040009

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.

- Embedded Packet Capture (EPC) is not supported on NCS 4200 routers.
- 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
```

- For VCoP, only SFP-T3F-SATOP-I is 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 disk space of 2 MB is required in the boot flash memory file system for a successful ROMMON auto upgrade process. For a disk space 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.



CHAPTER 2

What's New for Cisco IOS XE 17.13.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 17.13.1, on page 5](#)
- [What's New in Software for Cisco IOS XE 17.13.1, on page 5](#)

What's New in Hardware for Cisco IOS XE 17.13.1

There are no new hardware features for this release.

What's New in Software for Cisco IOS XE 17.13.1

Feature	Description
T1/E1 CEM Interface Module	
Framed SAToP System BERT	You can configure SATOP system BERT with framing under CEM circuits on T1 or E1 interfaces and verify if the BERT is stable and transmitted end-to-end.
User-defined Remote Loopback on T1 Interfaces	You can customize the loopback codes on T1 in a 16-bit format in contrast to the standard 6-bit loop code on the 48-port T1 interface module.



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 17.13.1, on page 7](#)
- [Open Caveats – Cisco IOS XE 17.13.1, on page 8](#)
- [Cisco Bug Search Tool, on page 8](#)

Resolved Caveats – Cisco IOS XE 17.13.1

Identifier	Headline
CSCwf07736	CEM interface counters momentarily report error when x21 xconnect is cleared and re-established.
CSCwh30217	With rate of OC12 we see "threshold sf-ber 3" getting added under show run command.
CSCwf86864	CEM traffic flow is dropped in one direction when DEI bit set.

Open Caveats – Cisco IOS XE 17.13.1

Identifier	Headline
CSCwh75614	Increased CPU after upgrading router to 17.6.3 from 16.9.4 when 1000 SLM/DMM sessions are configured.
CSCwh69286	Support required for LF and RF on Ethernet interfaces.
CSCwh82358	Service instance IDs of integers 4001-5000 is not supported.

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>