



# 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](http://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 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.

## 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](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](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](mailto: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](mailto:accessibility@cisco.com).

