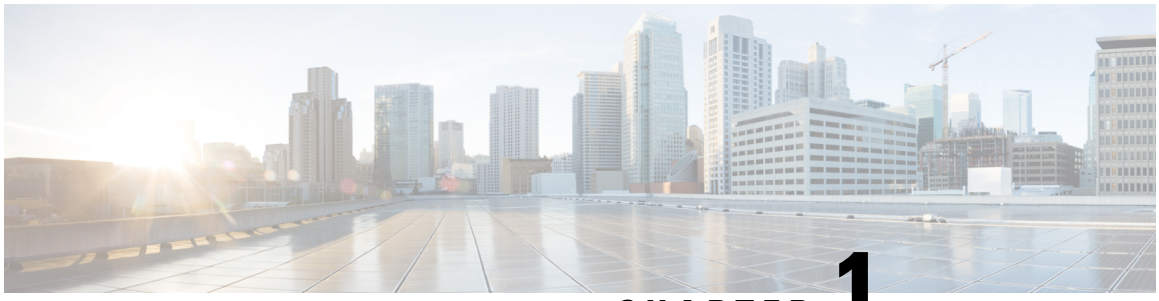
Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE 17.15.x

First Published: 2024-08-14

Last Modified: 2025-05-29

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

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(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 ont 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 frmware upgrade.

Bundled FPGA Versions

The following are HoFPGA versions bundled in the IOS for 17.15.x release:

- NCS4201—0X0004001b (15.6(57r)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:

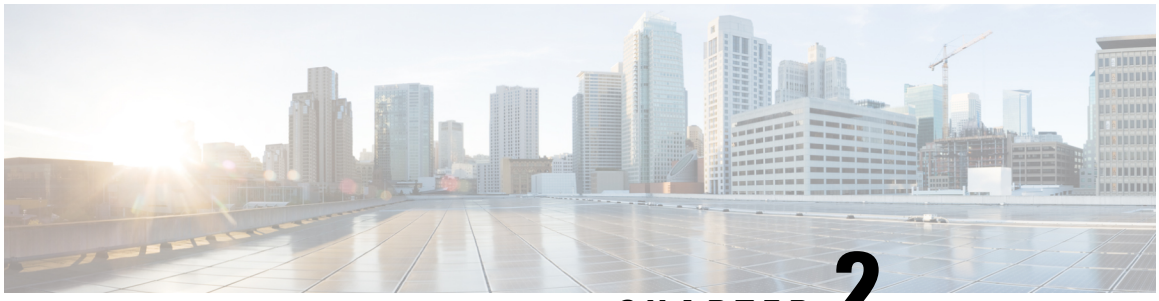
```
Speed is configured. Remove speed configuration before enabling auto-negotiation
```

- 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 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.



CHAPTER 2

What's New for Cisco IOS XE 17.15.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 17.15.3b

There are no new hardware features introduced for this release.

What's New in Software for Cisco IOS XE 17.15.3b

Feature	Description
IP Addressing	
Optimizing security and CPU utilization using software ACL in VRF traffic management	The Software ACL (SW ACL) is a platform-specific feature designed to control Layer 3 VRF traffic, such as ICMP, SSH, and Telnet, by managing traffic punted to the CPU. This feature enhances security and optimizes CPU utilization by allowing only explicitly permitted traffic to reach the CPU. The software ACLs enhances reliable and secure VRF-based services in enterprise networks and service provider networks. Command introduced: **platform sw_acl enable interface {icmp | ssh | telnet}**
MPLS	

Feature	Description
Support for Co-routed Inter-area Flex-LSP Tunnels in Point-to-Point OSPF network	Co-routed Flex LSP tunnels now support an inter-area and multiple areas in a Point-to-Point OSPF network. For example, in an inter-area OSPF network, both the head-end or tail-end for a bidirectional LSPs that are in different areas learn the network topology and perform the automatic path redundancy when there is a network link failure.

What's New in Hardware for Cisco IOS XE 17.15.2

There are no new hardware features introduced for this release.

What's New in Software for Cisco IOS XE 17.15.2

Feature	Description
Chassis	
NCCS 3GPP IP Specification Compliance for Interfaces	The router adheres to and complies with the IP specification guidelines as outlined by the National Centre for Communication Security (NCCS) certification, which is based on the 3rd Generation Partnership Project (3GPP) standards. This compliance ensures that the router meets rigorous security and performance benchmarks, providing users with a reliable and secure networking solution that aligns with industry best practices and regulatory requirements.
SNMP Dying Gasp support over IPv6 BGP Labeled Unicast Network	In addition to IPv4, SNMP dying gasp over FPGA is now extended to IPv6 BGP-Labeled Unicast (BGP-LU) network scenarios. This enhancement allows administrators to maintain and monitor their networks more effectively and robustly, ensuring reliable notification and management of critical network events across both IPv4 and IPv6 environments.

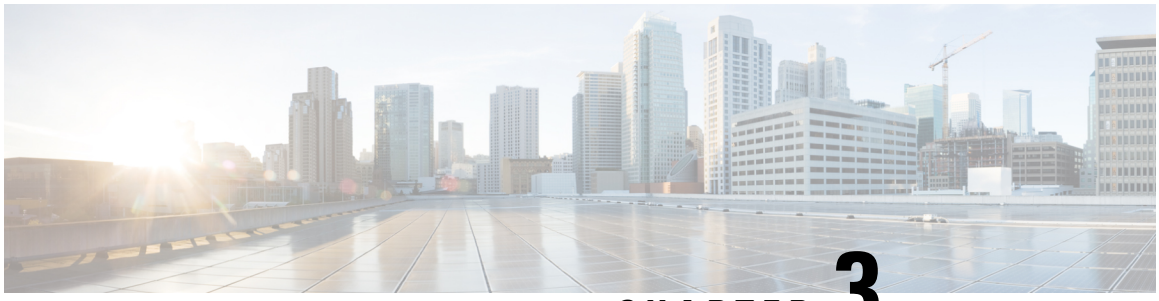
What's New in Hardware for Cisco IOS XE 17.15.1

Optics	Description
Management Port LED Status Indicators	The right LED indicator for the management port on the router now displays the link status and activity of the management port. You can monitor and troubleshoot the status and activity of the management port more effectively when the LED indicator turns green or in the Off state. For more details on the link status and activity, see the CPU Management Port LED Indication table.

What's New in Software for Cisco IOS XE 17.15.1

Feature	Description
Alarm Configuring and Monitoring	
SONET Alarms for APS	• With Automatic Protection Switching (APS), SONET alarms soaking as per the recommendation from GR-253. • Alarm is raised or cleared during APS manual, force, and lock out switch actions. • When traffic is switched to an alternate link in the APS group, the severity of the alarms is affected based on service impact.
SD-BER and SF -BER Alarms for T1/E1 and T3/E3 services	Signal Failure-Bit Error Rate (SF-BER) and Signal Degrade-BER (SD-BER) alarms are declared when there is a signal failure or signal degradation that happens in the traffic. These alarms may be raised when the error rate of a given entity exceeds the user-configured BER threshold value. This helps the administrator to take corrective actions.
CEM OCx	
DDS DS0 Remote Latching Loopback	DS0 loopback is used for testing and troubleshooting the T1 or E1, T3 or E3, and OCx channel over PSN. You can configure DS0 loopback on these controllers for remote devices.
Protection Switching Count for Protected SONET Interface	In SONET with redundancy, an Automatic protection switching (APS) occurs between working and standby protection networks due to reasons like a circuit failure. Whenever the switching happens, the switching count is tracked using a Protection Switching Count (PSC) parameter. Depending on the PSC count, you can debug the network to identify the reason for extensive switching and work on the corrective actions.
TCAM and NFT Commands	

Feature	Description
TCAM and NFT Commands	New commands have been introduced for the Ternary Content-Addressable Memory (TCAM) and NFT. **TCAM** You can now view the Ternary Content-Addressable Memory (TCAM) utilization for each control plane TCAM entry. Command: show platform hardware pp active tcam utilization control-plane-sessions **NFT** • You can now enable the collection of the packets punted to the CPU from the NFT hash table. Command: platform nft-summarization enable • Once the above command is enabled, you can use a timer to clean up the NFT hash table. Command: platform nft-summarization timer-value • You can view a summary of the packets punted to the CPU from the NFT hash table. Command: show platform hardware pp active infrastructure pi nft summary



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 17.15.3b

Identifier	Headline
CSCwm82342	Post reload HSRP is stuck in Init state and shows interface down
CSCwn94246	XCVR incompatible alarm missing without Sonet controller configurations.
CSCwn41240	Observed nnframed T1 as none and not shown in running-config under T3 controller.
CSCwo10841	XCVR incompatible alarm not asserted in Bay0 sonet controller cards

Open Caveats – Cisco IOS XE 17.15.3b

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE 17.15.2

Identifier	Headline
CSCwm91197	Silent reload of 3GMS IM due to PCI transaction failure.
CSCwm86214	LDP session flap causes memory leak for EMPLS3LD which leads to RSP crash.

Open Caveats – Cisco IOS XE 17.15.2

Identifier	Headline
CSCwm63093	Protocol or interface configuration from start or run file is missing after reload issue.
CSCwm04031	17.9.2a-Both active and standby RSP's OAM or CFM configurations automatically changed after a reload.

Resolved Caveats – Cisco IOS XE 17.15.1

Identifier	Headline
CSCwi76112	Message to be displayed for M13 framing when configured with clear-channel
CSCwi60730	Speed LED status is not correct when sonet/sdh mode is configured
CSCwi33111	T1: Sev changes back from major to minor after IM OIR.
CSCwj06370	Serial cease traffic when configuring module other port
CSCwj05647	3GMS Serial interface protocol down with specific Modem
CSCwj12451	Update 2^20-O151 QRSS bert help string with QRSS Keyword
CSCwj44502	DCR clocking fails to get acquired on the with sts1-E mode
CSCwj99522	Need to support dtr not-used CLI in RS232 transparent mode
CSCwi92203	Channelized DS3: RAI is propagating to all DS1's when DS3 RAI is asserted

Open Caveats – Cisco IOS XE 17.15.1

Identifier	Headline
CSCwk46171	Enabling T1/E1 TPoP causes latency for control plane packets
CSCwk58917	L-bit propogation not enabled for LOF alarm after framing change with framed SAToP
CSCwk02087	BFD stuck in INIT state for interface Te0/0/0 & Te0/4/3
CSCwh75614	Increased CPU after upgrading router to 17.6.3 from 16.9.4 when 1000 SLM/DMM sessions are configured
CSCwj60760	Confd process not in Started State in 5 mins after netconf-yang config is done
CSCwk27810	After reconfiguring second synce source the QL-failed for that source interface and ranking also 254

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