Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE Dublin 17.12.x

First Published: 2023-06-26

Last Modified: 2025-02-13

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 17.12.1 release:

- NCS4201—0X0004001b (15.6(56r)S)

- NCS4202
  - BFD—0X00040009
  - Netflow—0X00040009

The following is the CEM FPGA version:

- NCS4202—0X00040009

The following are HoFPGA versions bundled in the IOS for 17.12.3 release:

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

The following is the CEM FPGA version:

- NCS4202—0X00040009

The following are HoFPGA versions bundled in the IOS for 17.12.4 release:

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

The following is the CEM FPGA version:

- NCS4202—0X00040009

The following are HoFPGA versions bundled in the IOS for 17.12.5 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.

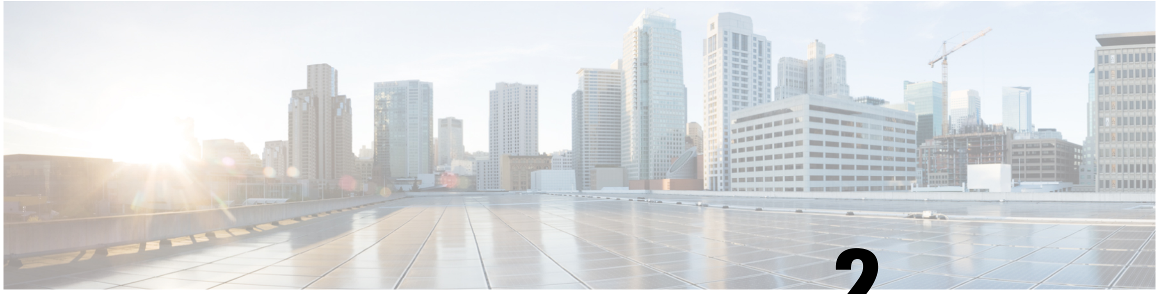
- Embedded Packet Capture (EPC) is not supported on NCS 4200 routers.
- The **default** *command-name*command is used to default the parameters under that interface. However, when speed is configured on the interface, the following error is displayed:

  ```
  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 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 Dublin 17.12.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 Dublin 17.12.5

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Dublin 17.12.5

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Dublin 17.12.4

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Dublin 17.12.4

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Dublin 17.12.3

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Dublin 17.12.3

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Dublin 17.12.2a

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Dublin 17.12.2a

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Dublin 17.12.1

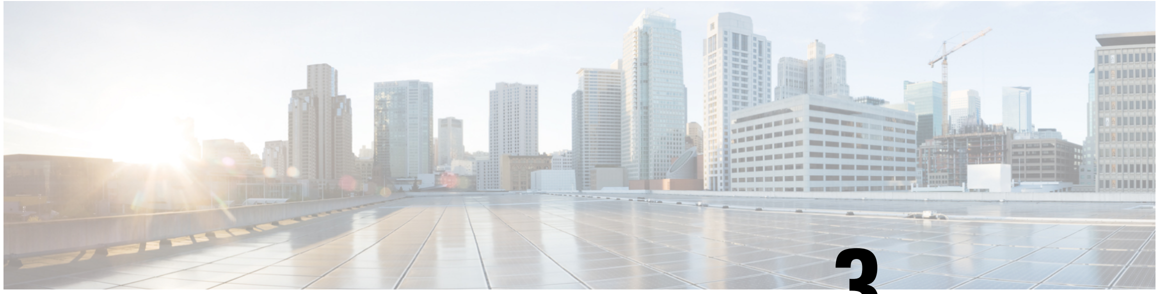
Table 1: Supported Optics

Feature	Description
Optics	This release launches the following new optics on selective hardware within the product portfolio. For details refer to the Transceiver Module Group (TMG) Compatibility Matrix. • Cisco Data SFP modules • ONS-SI-GE-EX

What's New in Software for Cisco IOS XE Dublin 17.12.1

Feature	Description
Carrier Ethernet	
Service Instance as Track Client	Track can be configured to check for reachability to IBR(Upstream router). If IBR is not reachable, the service instance is kept in admin down state. This avoids traffic drop until the route is installed which optimizes the convergence. Currently, IOS XE platforms do not have options to shutdown EFP based on track reachability.
CEM	

Feature	Description
CEM Description Command	You can add description for a cem group up to 200 characters using the **description** command.
Layer 2	
MACsec support with PTP for 1GE NCS4200-1T16G-PS Interface Module	You can now configure MACsec support with Precision Time Protocol (PTP) packets for mitigating security vulnerabilities on a router.



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 Dublin 17.12.5

Identifier	Headline
CSCwk46171	Enabling T1/E1 TPoP causes latency for control plane packets.
CSCwm91197	Silent reload of 3GMS IM due to PCI transaction failure.
CSCwm00642	RSP reboots while configuring CEM IDs on ACR.

Identifier	Headline
CSCwm86214	LDP session flap causes memory leak for EMPLS3LD which leads to RSP crash.
CSCwk58917	L-bit propogation not enabled for LOF alarm after T1/E1 framing change with framed SAToP.

Open Caveats – Cisco IOS XE Dublin 17.12.5

Identifier	Headline
CSCwk99487	Silent reload happens on router.
CSCwi76112	Message to be displayed for M13 framing when configured with clear-channel.

Resolved Caveats – Cisco IOS XE Dublin 17.12.4

Identifier	Headline
CSCwj71820	L2VPN pseudowire configuration is causing the GNMI state go down

Open Caveats – Cisco IOS XE Dublin 17.12.4

Identifier	Headline
CSCwf32880	QoS performance enhancement for tagged EVC
CSCwi64206	Port LED status glows in green color even after the peer end connection is removed & same vice versa

Resolved Caveats – Cisco IOS XE Dublin 17.12.3

Identifier	Headline
CSCwh88274	Unable to remove service-policy from from standby member link
CSCwi75499	Lost CEM circuit configuration after reboot
CSCwh68394	Unable to remove the service instance under interface
CSCwh85621	The **show platform ha cef ip/ipv6** command is displaying partial output for POCH interface
CSCwi85575	The router drops Wake on LAN (WoL) packet for directly connected interface

Identifier	Headline
CSCwh57819	IP services are down in the device after each reboot
CSCwh84408	The process pubd is not running in NCS4201-02 and RSP2 device
CSCwj01024	ISIS: Counter for the number of redistributed routes does not get decremented

Open Caveats – Cisco IOS XE Dublin 17.12.3

Identifier	Headline
CSCwh17987	NCS4201-02: traffic drop seen when BW on the Gig interface is changed to 100 Mb with MTU beyond 5000
CSCwj05647	3GMS Serial interface protocol down with specific Modem
CSCwh66210	Netconf RPC failed to apply if increase mpls MTU limit to 9644 bytes
CSCwj06370	Serial cease traffic when configuring module other port
CSCwi64206	Port LED status glows in green color even after the peer end connection is removed and same vice versa
CSCwh59032	CPE SIT: Data structure error pointing to rsvp-db during TE FRR
CSCwh75614	Increased CPU after upgrading router to 17.6.3 from 16.9.4 when 1000 SLM/DMM sessions are configured

Resolved Caveats – Cisco IOS XE Dublin 17.12.2a

Identifier	Headline
CSCwf81523	OCX: traceback seen IOSXE_RP_SPA-3-IOMD_CONFIG_FAIL: when mode sonet is configured.
CSCwh30217	NCS4200-3GMS: With rate of OC-12, the threshold sf-ber 3 is added under the `show running-config` command.
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability.
CSCwh04884	VC Down due to control-word negotiation
CSCwf79476	When certificate issue `show platform sudi certificate sign nonce xxxx`, Flaps L3 interfaces
CSCwh75169	ISIS: Redistribution prefix threshold is reached with lesser prefixes.
CSCwf16577	BFD session down alarm does not clear after fault recovery.

Open Caveats – Cisco IOS XE Dublin 17.12.2a

Identifier	Headline
CSCwh75614	IP SLA Multicast configuration Not Working
CSCwh82358	Service Instance IDs of integers 4001-5000 is not supported.
CSCuv05226	VRF is not deleted after replacing default configuration.
CSCwh66210	Netconf RPC failed to apply if MPLS MTU limit is increased to 9644 bytes.
CSCwh68394	Unable to remove the service instance under interface.
CSCwh89032	Remove vulnerability in open port.

Resolved Caveats – Cisco IOS XE Dublin 17.12.1

Identifier	Headline
CSCwd78618	IMASER14A/S does not boot.
CSCwe98227	The "show version" does not display details of T1/E1 interfaces for 8D and 32D IMs.
CSCwd90840	Mcast data traffic is getting dropped over vpls.
CSCwe38904	Frame loss seen for 64 bytes packet size for rate step 2333333/all kbps.
CSCwf42164	No snmp trap link-status get re-added after IM reload.
CSCwf49426	PAIS alarm get reported after IM OIR.
CSCwf48343	Display issue when Label pointing in LB object in BGP-PIC edge case.
CSCwd85267	FR Port mode - show interface CLI does not display FR PW statistics.
CSCwd25376	Loopback local on 3GMS IM causing BIP B2 counters increment under show controller CLI.
CSCwe54549	SFP not detected due to checksum error.
CSCwe10460	Power sensor threshold warning alarms in EPNM.
CSCwe58324	Node reload observed after routing change in core.
CSCvy81362	Controllers are down due to LP-LOP alarm After CE reboots.
CSCwf67803	DS3_ADMIN_DOWN gets cleared after IM OIR and displaying LINK_DOWN alarm in 3GMS.
CSCwd46121	Time stamp issue on Transparent clock for 1G PORTS.

Identifier	Headline
CSCwe38959	rs232 ASYNC PW service with full scale seeing packet and byte drops intermittently.
CSCwe13024	RSP2: All readings for Power supply unit reflect as zero though the unit is functional.
CSCwd67723	In IMA32D/IMA8D card, sometimes change in E1 controller config(after ctrlr flap)results in IM reboot.
CSCwe27336	Cylon error logs during reload.
CSCwe19162	After SSO: False Alarm on CNAAP.
CSCwe55191	ISIS neighbors flap during switchover when authentication is enabled.
CSCwe95820	VRF Static Route Redistribution into EIGRP fails.
CSCwe53345	External R1 10M is not selected after double SSO with GNSS.
CSCwd66936	RSP2 UDP pseudowire stuck in activating.
CSCwe36122	ISIS crash when performing TI-LFA calculation.
CSCwe27155	Seen traffic drop with BDI shut (IP_FRR configs).

Open Caveats – Cisco IOS XE Dublin 17.12.1

Identifier	Headline
CSCwf23533	PTP-G8275.1 Profile - High Offset Seen on BC th data traffic.
CSCwf71463	With traffic ON, when speed lowered on ASYNC port, SYNC port CEM traffic gets impacted.
CSCwf65076	The isis hello-interval minimal configuration causes ASIC lock.
CSCwf18420	LLDP does not announce dynamically assigned VLAN.
CSCwf68400	RSP3:<group>0</group> additional value gets added during fetch, applying the same config fails.

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