Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE Cupertino 17.8.x

First Published: 2022-04-08

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.

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(48r)S
- NCS4202—15.6(46r)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 17.8.1 release:

- NCS4201—0X0004001b
- NCS4202
  - BFD—0X0003001e
  - Netflow—0X0003001e

The following is the CEM FPGA version:

- NCS4202—0x10020076

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 Cupertino 17.8.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 Cupertino 17.8.x

Feature	Description
SFP Modules	
New SFP Modules	This release introduces support for the following SFP module: • ONS-SI-GE-SX For more information, see the Cisco Network Convergence System Routers NCS 4201-02 Series Optics Matrix.

What's New in Software for Cisco IOS XE Cupertino 17.8.x

Feature	Description
Carrier Ethernet	
Increase Maximum MTU Size	Maximum Transmission Unit (MTU) is increased to a maximum of 9670 bytes on the Cisco RSP2 module. You can configure the MTU bytes using the **mtu** *bytes* command.
CEM	

Feature	Description
Frame Relay Support for IP Interworking	Support for frame relay encapsulation on iMSG serial interface for the following interface modules: • 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 • NCS 4200 Combo 8-Port SFP GE and 1-Port 10 GE 20G interface module Frame Relay being a streamlined protocol facilitates higher performance and greater efficiency.
NCS4200-48T1E1-CE support in NCS4202	The router supports the following features for the 48-Port T1/E1 Circuit Emulation (CEM) interface module: • Basic mode, and T1 or E1 controller required configurations • CEM clocking, ACR, and DCR • CEM pseudowires such as Structure-Agnostic TDM over Packet (SATOP) and Circuit Emulation over Packet-Switched Network (CESoPSN) • BERT, loopback, and alarms • Performance monitoring The support for the interface module provides cost-effective delivery of CEM over a packet-based network (MPLS).
IP Routing: BGP	
Outbound Route Filtering (ORF) Support for BGP Labeled Unicast	This feature uses BGP ORF send and receive capabilities to minimize the number of BGP updates that are sent between BGP peers. It can also filter out unwanted routing updates at the source to reduce the amount of system resources that are required for generating and processing routing updates.
Layer 2	
Mac Address Limiting Per Bridge Domain	This feature restricts the number of MAC addresses that the router learns in a bridge-domain on an EFP, pseudowire or trunk EFP to a specified number. Use the feature to enable warning and limit actions when a violation occurs.
Support for Ethernet Data Plane Loopback on Bundle Interface	This feature enables ethernet data plane loopback on bundle interfaces.
Y.1564 and EDPL support on dot1ad	This feature allows Y.1564 and EDPL to be supported on interfaces that are configured with 802.1ad encapsulation. The following commands are introduced: - **inner-eth-type** - **outer-eth-type**
Cisco IOS Multiprotocol Label Switching Command Reference	

Feature	Description
Long Service Name	The description command in the **l2vpn xconnect** configuration has been modified to support a maximum of 240 characters. In addition, a new description command, which supports 240 characters, has been added in the **connect connection-name** configuration. You can set this by executing the **description** command in the configuration mode. This implementation is useful for administrative purposes.
YANG Native Config Model Hardening: Cisco-IOS-XE-wccp.yang	Support for YANG Native Config Model Hardening: Cisco-IOS-XE-wccp.yang is introduced in this release.
Sensitive Data Erase	Support for sensitive data erase is introduced in this 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 Cupertino 17.7.1

Identifier	Headline
CSCvz79672	HQoS on egress TenGig interface is not working properly
CSCvy78284	Router will crash when zeroised RSA key is regenerated
CSCwa33365	SNMP polling for traffic stats displays wrong values for all interface
CSCwa14057	'cylon_mgr_F0-0.log' tracelog is filling bootflash continuously
CSCwa41670	Cylon_mgr crash @adjmgr_get_nh_flag with 16.9.4 image
CSCwa04795	Interfaces are showing up in SNMP polling while associated Hardware Does not Exists on System
CSCvy92074	MTU programming for MPLS L2 VC may fail after interface flaps

Identifier	Headline
CSCwa41638	MAC Table and L2VPN EVPN Table out of sync

Open Caveats – Cisco IOS XE Cupertino 17.8.1

Identifier	Headline
CSCvz65726	Post SSO with QoS OHA counters stop working
CSCwa33548	We observed traffic issue with latest labels &bi-directional traffic is not working and drop is seen

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