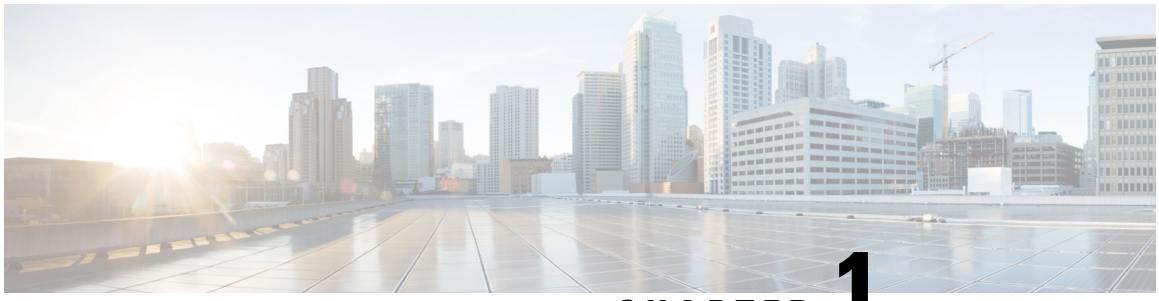
Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE Cupertino 17.9.x

First Published: 2022-12-04

Last Modified: 2024-09-16

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



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

The following are HoFPGA versions bundled in the IOS for 17.9.1 release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202—0X00040009 (15.6(54r)S)
  - BFD—0X00040009
  - Netflow—0X00020008

The following are HoFPGA versions bundled in the IOS for 17.9.2a release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202—0X00040009 (15.6(54r)S)
  - BFD—0X00040009
  - Netflow—0X00020008

The following are HoFPGA versions bundled in the IOS for 17.9.3 release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202—0X00040009 (15.6(54r)S)
  - BFD—0X00040009
  - Netflow—0X00020008

The following are HoFPGA versions bundled in the IOS for 17.9.4 release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202—0X00040009 (15.6(54r)S)
  - BFD—0X00040009
  - Netflow—0X00020008

The following are HoFPGA versions bundled in the IOS for 17.9.5a release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202—0X00040009 (15.6(54r)S)
  - BFD—0X00040009
  - Netflow—0X00020008

The following are HoFPGA versions bundled in the IOS for 17.9.6 release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202—0X00040009 (15.6(54r)S)
  - BFD—0X00040009
  - Netflow—0X00020008

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 17.9.1 release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202—0X00040009 (15.6(54r)S)
  - BFD—0X00040009
  - Netflow—0X00020008

The following are HoFPGA versions bundled in the IOS for 17.9.2a release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202—0X00040009 (15.6(54r)S)

- BFD—0X00040009
- Netflow—0X00020008

The following are HoFPGA versions bundled in the IOS for 17.9.3 release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202—0X00040009 (15.6(54r)S)
  - BFD—0X00040009
  - Netflow—0X00020008

The following are HoFPGA versions bundled in the IOS for 17.9.4a release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202—0X00040009 (15.6(54r)S)
  - BFD—0X00040009
  - Netflow—0X00020008

The following are HoFPGA versions bundled in the IOS for 17.9.5a release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202—0X00040009 (15.6(54r)S)
  - BFD—0X00040009
  - Netflow—0X00020008

The following are HoFPGA versions bundled in the IOS for 17.9.6 release:

- NCS4201—0X0004001b (15.6(56r)S)
- NCS4202—0X00040009 (15.6(54r)S)
  - BFD—0X00040009
  - Netflow—0X00020008

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.

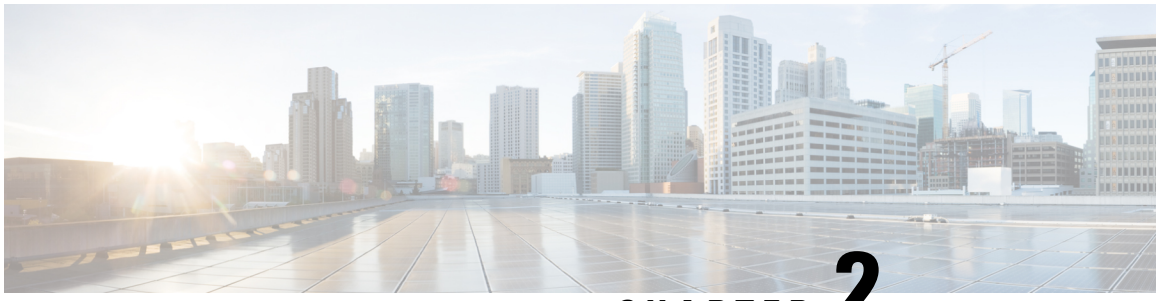
- Embedded Packet Capture (EPC) is not supported on NCS 4200 routers.
- The **default** *command-name*command is used to default the parameters under that interface. However, when speed is configured on the interface, the following error is displayed:

```
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 17.9.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 Software for Cisco IOS XE Cupertino 17.9.6

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Cupertino 17.9.6

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Cupertino 17.9.5a

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Cupertino 17.9.5a

There are no new hardware features in this release.

What's New in Hardware for Cisco IOS XE Cupertino 17.9.4a

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Cupertino 17.9.4a

There are no new features in this release. This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see cisco-sa-iosxe-webui-privesc-j22SaA4z.

What's New in Hardware for Cisco IOS XE Cupertino 17.9.4

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Cupertino 17.9.4

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Cupertino 17.9.3

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Cupertino 17.9.3

There are no new software features in this release.

What's New in Software for Cisco IOS XE Cupertino 17.9.2a

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Cupertino 17.9.2a

There are no new hardware features in this release.

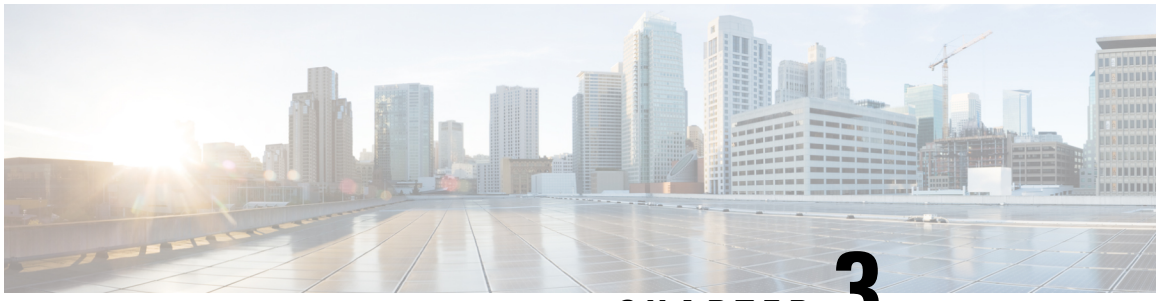
What's New in Software for Cisco IOS XE Cupertino 17.9.1

Feature	Description
Carrier Ethernet	
Application of QoS Policies on ITU-T Y.1731 Egress Packets	You can now apply QoS policies on Y.1731 egress packets. Operations, Administration, and Maintenance (OAM) functions and mechanisms for Ethernet-based networks are defined in ITU-T Y.1731. With this implementation, you can prioritize OAM traffic; for example, prioritizing operational information used to detect faults and determining network performance.
Layer 2 Control Protocol Enhancements	Layer 2 Control Protocols (L2CP) propagate the MAC address control information to determine which parts of a network the router should forward, tunnel, peer, or discard information. • MRP Block • Cisco BPDU • Cisco STP UplinkFast • Cisco CFM
Custom Idle Pattern	You can configure idle pattern manually on CEM circuits and verify if it's stable and transmitted to the other end in alarm conditions. You can configure on all CEM PWs in a T1/E1 circuit. Supported on the following IMs on CESoPSN circuits with both partial and full time slots. • 48-port T1/E1 CEM Interface Module • 48-port T3/E3 CEM Interface Module • 1-port OC481/ 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 These idle pattern numbers are used for tracking purposes.
MPLS Basic	
Support for Co-routed Inter-area Flex-LSP Tunnels	Flex LSPs (also called Associated Bidirectional LSPs) now support inter-area co-routed tunnels. With this implementation, we meet the specific requirements of network operators to create on-demand tunnels by defining an explicit path across different areas.
System Logging	

Feature	Description
No Service Password Recovery	This feature provides additional security by removing all user files from bootflash during factory reset. It prevents the malicious users from accessing configuration files stored in bootflash. This feature is applicable for NCS 4201 and NCS 4202 routers.
YANG Model Support for QoS Service Group	Cisco YANG now supports QoS Service Groups. Service-Groups allow you to add service instances to groups and apply service policies. You can configure the definition of the service-group and apply the service-group to an interface. With this implementation, you can quickly deploy QoS mechanisms, such as creating a class for email traffic.
IPv6: RFC 8200 Compliance	Improvements have been made to the Cisco IOS XE platforms to maintain compliance with IETF standards as specified for the Internet Protocol, Version 6 (IPv6) in RFC 8200. The enhancements bring in improved security and better handling of IP packets with fragments.
TPoP T1/E1 clock status display update	Starting with release Cisco IOS XE Cupertino 17.9.1, TPoP T1/E1 clock status is accurately displayed in the recovered clock status output.
Show Tech-Support Enhancements	
Show Tech-Support Enhancements	The **show tech-support** now supports generic commands to provide better debuggability. The **show tech-support platform cef** command now displays IPv4 address information. For more information, see Cisco IOS Configuration Fundamentals Command Reference.

What's New in Hardware for Cisco IOS XE Cupertino 17.9.1

There are no new hardware features 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 17.9.6

Identifier	Headline
CSCwi75499	Lost CEM Circuit Configuration After Reboot

Identifier	Headline
CSCwj82056	Smart Licensing is not getting auto-register while upgarding the node.
CSCwi64206	Port LED status glows in green color even after the peer end connection is removed & same vice versa
CSCwj58921	[SVSP-893] Node adds a duplicate entry for BGP path in table whenever route-refresh is done

Open Caveats – Cisco IOS XE Cupertino 17.9.6

Identifier	Headline
CSCwk48598	PSU/FAN is showing as N/A after silent reload
CSCwk99487	Silent reload
CSCwk71598	Gratuitous ARP looping in REP Port-channel issue after upgrade/reload of the device

Resolved Caveats – Cisco IOS XE Cupertino 17.9.5a

Identifier	Headline
CSCwf07736	cem interface counters momentarily report error when x21 xconnect is cleared and re-established
CSCwi41800	Block end users from removing a GRANDPARENT policy-map if the policy-map is attached to an interface
CSCwb01284	ASR 900 Series PTP Sync degraded on Tester after primary PTP source failover to secondary
CSCwe24919	RJIL ASR-920 issue: both Power Supply is showing fail state while LED is Green

Open Caveats – Cisco IOS XE Cupertino 17.9.5a

Identifier	Headline
CSCwd46121	Time stamp issue on Transparent clock for 1G PORTS
CSCwd23704	ASR920: Warning message seen on enabling scaleipv6 sdm template.
CSCwd89451	ASR920/NCS4202 doesn't forward IPv6 packets with src address 0:0:0:0:0:0:0:1111

Resolved Caveats – Cisco IOS XE Cupertino 17.9.4a

Identifier	Headline
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

Open Caveats – Cisco IOS XE Cupertino 17.9.4a

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE Cupertino 17.9.4

Identifier	Headline
CSCwe38959	rs232 ASYNC PW service with full scale seeing packet and byte drops intermittently.
CSCwd90840	mcast data traffic is getting dropped over vpls.
CSCwe54549	SFP not detected due to checksum error.
CSCvy81362	Controllers are down due to LP-LOP alarm After CE reboots.
CSCwe34672	High CPU on ptp_uea process.
CSCwd67723	In IMA32D/IMA8D card, sometimes change in E1 controller config(after ctrlr flap)results in IM reboot.
CSCwd85267	FR Port mode - show interface CLI does not display FR PW statistics.
CSCwe10460	Power sensor threshold warning alarms in EPNM.

Open Caveats – Cisco IOS XE Cupertino 17.9.4

Identifier	Headline
CSCwd05362	Performance issue on router platform.
CSCwd67723	In IMA32D/IMA8D card, sometimes change in E1 controller config(after ctrlr flap)results in IM reboot.
CSCwe13024	All readings for Power supply unit reflect as zero though the unit is functional.
CSCwe27155	Seen traffic drop with BDI shut (IP_FRR configs).

Resolved Caveats – Cisco IOS XE Cupertino 17.9.3

Identifier	Headline
CSCwc76004	Wrong timestamp in TWAMP test packet with PTP active
CSCwd57471	Change in BGP ORF prefix-filter not being advertised from XE to XR node
CSCwb77093	next hop self does changes automatically on VRF lite and ipv4
CSCwd06972	IOS-XE 17.x - user password not saved if user attribute list is configured
CSCwd58396	NETCONF: Failed sync between Running configs and Candidate database
CSCwc55520	Traceback and IDB leak noticed when a RSP3 setup performs a switchover

Open Caveats – Cisco IOS XE Cupertino 17.9.3

Identifier	Headline
CSCwc76004	Wrong timestamp in TWAMP test packet with PTP active
CSCwc93296	16.9.4/port Te0/0/10 went admin down after in successive reload
CSCwd76589	BGP On Change Notification not sent for BGP Dynamic Peers
CSCwc03907	ISIS SRLG to BGPLS export problems
CSCwd90908	NTP packets are sent from global VRF with a source IP configured on service VRF interface

Resolved Caveats – Cisco IOS XE Cupertino 17.9.2a

Identifier	Description
CSCwc84627	Router reboots continously for a PCIE bus error
CSCwb77396	G.8032: Ring brief output does not display the Block port flag in Idle state
CSCwc21402	Invalid BGP update when add-paths negotiated only for label (SAFI 4) and not unicast (SAFI1)
CSCwc67367	Seeing traffic issues after clearing ISIS with **SRTE_ODN_ISIS_Flex_Algo** configs

Open Caveats – Cisco IOS XE Cupertino 17.9.2a

Identifier	Description
CSCwc93296	Port Te0/0/10 reports admin down after successive reloads
CSCwc79322	Memory leak on **ptpd_uea** process
CSCwd19387	PTP time source changes to Internal Oscillator impacting services
CSCwd46121	Time stamp issue on Transparent clock for 1G PORTS process
CSCwc54860	EIGRP down authentication issues after ugprading from 17.3 to 17.6
CSCwb78907	DS3_RX_RAI is shown in both **facility-alarm** and **facility-condition status** commands
CSCwc23316	Command **show snmp mib ifmib ifindex detail [IntName]** truncated when is more than 32 characters

Resolved Caveats – Cisco IOS XE Cupertino 17.9.1

Identifier	Headline
CSCwa33548	We observed traffic issue with latest labels and bi-directional traffic is not working and drop is seen
CSCvy78284	Router crashes when zeroised RSA key is regenerated
CSCwa52959	TPOP T1/E1 : Clock status to be corrected for alarm condition
CSCwa16189	SNMP traps are seen continuously in SNMP server with MPLS-TE configuration
CSCvz65726	Post SSO with Qos OHA counters stop works
CSCvv16943	Uea-iomd phase2 IM FPD ugprade commit to polaris_dev
CSCvw17894	Exception for weak algorithm options for SNMP does not work
CSCwb01224	Multihop BFD transit packets getting droppedn on router after upgrade to 17.3.3
CSCwb01940	Router drops L2 multicast traffic upon REP topology change
CSCwa41638	Router MAC Table and L2VPN EVPN Table out of sync

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