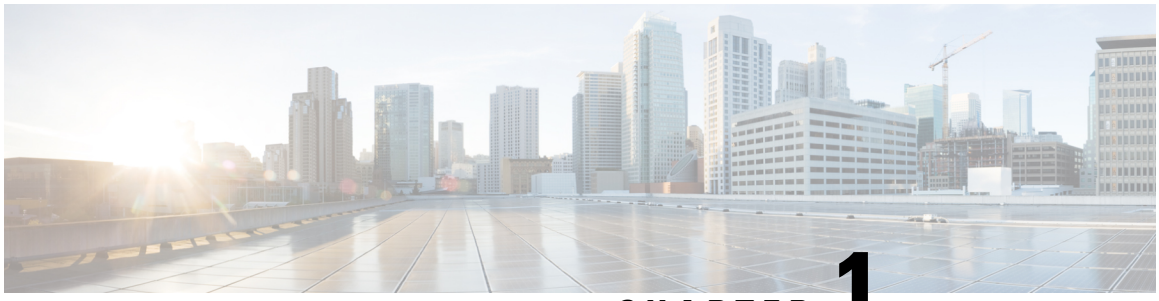
Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE Dublin 17.11.x

First Published: 2023-04-07

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

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(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:

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

The following is the CEM FPGA version:

- NCS4202—0x10020076

The following are HoFPGA versions bundled in the IOS for 17.7.1 release:

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

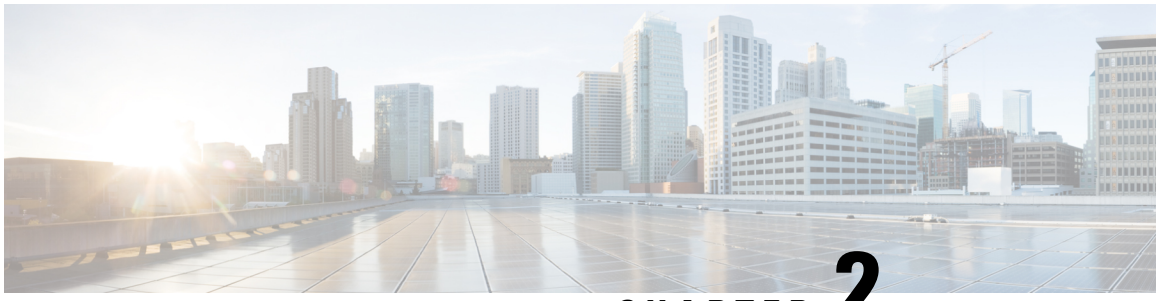
- Embedded Packet Capture (EPC) is not supported on NCS 4200 routers.
- The **default** *command-name*command is used to default the parameters under that interface. However, when speed is configured on the interface, the following error is displayed:

```
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 17.11.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 17.11.1a

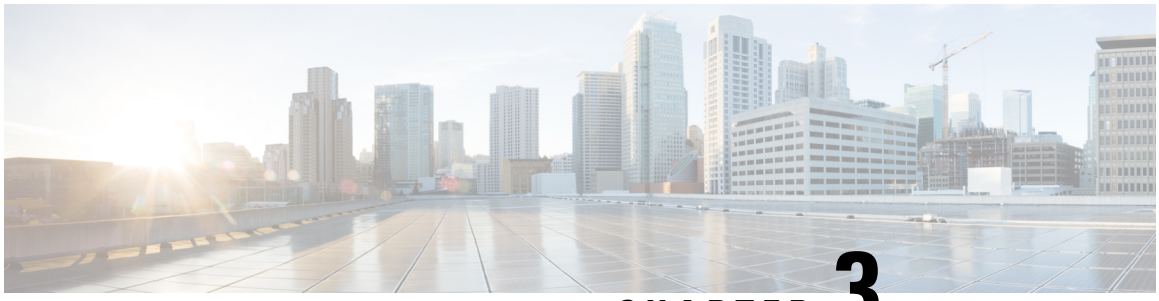
There are no new hardware features for this release.

What's New in Software for Cisco IOS XE Dublin 17.11.1a

Feature	Description
CEM	
Frame Relay Port Mode	Frame Relay (FR) port mode provides transport between two Provider Edge (PE) devices, where the complete FR frame is transported using the same encapsulation configured for the HDLC or FR pseudowire. On the PE device, the multiple FR Virtual Circuits (VCs) are carried over a single interface and the traffic is passed into a single transparent HDLC or FR pseudowire in an MPLS network. Thus with port mode, there are many-to-one mappings between multiple FR VCs and a pseudowire in a secure manner. You can configure HDLC or FR port mode on 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
Support for 3-in-24 BERT Patterns	• 48-port T1 or E1 interface module • 1-Port OC-48 or 4-Port OC-12/OC-3 interface module

Feature	Description
System CESoP NxDS0 BERT	You can configure BERT patterns at the DS0 level on the following interface modules for both the system and line directions. • 48-Port T1 or E1 CEM interface module • 48-Port T3 or E3 CEM interface module • 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 You can configure speed with bandwidth of 56 kbps or 64 kbps along with the BERT pattern. With DS0 level BERT configuration, you can verify the end-to-end connectivity.
Layer 3 Termination for Frame Relay	You can configure layer 3 termination on the Frame Relay (FR) and Multilink Frame Relay (MFR) sub interfaces for the following interface modules: • NCS4202-SA equipped with NCS4200-3GMS You can assign IP address on the FR or MFR sub interface and terminate the Layer 3 traffic where ever required in the network.
Timing and Synchronization	
NTP Support for IPv6 Networks	Network Time Protocol (NTP) synchronizes device clocks across networks to maintain system accuracy. In this release, NTP supports IPv6 multicast networks. The NTP server sends clock updates as multicast messages to the clients across IPv6 networks. As NTP packets are sent only to the intended clients, it reduces timing traffic in the network.
Software Activation	
No License Snapshot Support	License snapshot won't be generated starting from this release and the software relies only on the existing snapshot for any PAK license information.
Strong Crypto Algorithms	
Strong Crypto Algorithms	We strongly recommend stronger cryptographic algorithms instead of weak cryptographic algorithms, such as RSA keys of less than 2048 bits, MD5 for authentication, DES, and 3DES for encryption. Soon, such weak algorithms will no longer be allowed by default. An explicit configuration is required to continue using such weak algorithms. For SNMP v3 users with weak cryptographic properties, the SNMP operations to the device will fail, resulting in loss of management access to device through SNMP. Similarly, if the RSA key pair is not updated to be at least 2048 bits for SSH, the SSH server will be disabled, resulting in loss of remote access to the device through SSH. For more information on how to migrate to stronger cryptographic algorithms for SNMP, see the Field Notice Number: FN72509. For more information on how to migrate to stronger cryptographic algorithms for SSH, see Field Notice Number: FN72511.

Feature	Description
IP SLAs	
QoS for Y.1564 SADT External Sessions	Y.1564 Ethernet service activation test methodology now supports Ingress and Egress QoS policy configuration on interfaces. You can now measure QoS traffic throughput and loss using SADT external sessions on the ingress traffic. In earlier releases, Y.1564 supports egress QoS policy. With this enhancement, both SADT ingress and egress traffic can coexist on an interface.
Programmability	
gNMI Dial-Out Using gRPC Tunnel Service	This feature allows you to configure a network device (tunnel client) to register certain targets (preapproved services) with a gRPC tunnel server through the CLI. These targets are defined as ports on the network device. You can use the gRPC tunnel server to forward connections from external clients, such as gRPC Network Management Interface (gNMI)/gRPC Network Operations Interface (gNOI), to connect to the network device without establishing a direct connection. The following commands are introduced for the tunnel and target configurations respectively: • **gnxi grpctunnel destination** *server name* • **gnxi grpctunnel target**
YANG	
YANG Support for show l2vpn atom vc detail Command	The Cisco-IOS-XE-l2vpn-oper native model is a collection of YANG definitions for L2VPN services operational data. Additional leaves and lists are now supported in the following sensor path: **Cisco-IOS-XE-l2vpn-oper\l2vpn-oper-data\l2vpn-services\l2vpn-atom-vc-info** With this model, you can get detailed information, such as the L2VPN service name, service type, interface name, peer address, status, encapsulation type, virtual circuit ID, and packet information by using a NETCONF RPC. In earlier releases, you could perform this action by using the following CLI: **show l2vpn atom vc detail** **Note** There is existing YANG support for the following related CLIs in the **Cisco-IOS-XE-l2vpn-oper** native model: • **show l2vpn service xconnect peer peer_id vcid vcid** • **show l2vpn atom commands** YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/main/vendor/cisco/xe. Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same GitHub location highlights changes that have been made in the 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 Dublin 17.11.1a

Identifier	Headline
CSCwc80493	APS - K2 byte not reflecting proper value during LRDI and LAIS conditions.
CSCwd04198	A900-IMASER14A/S: when configurations are pasted in a specific order, line config is missing
CSCwc41115	APS 1+1 Uni - Tx K2 to reflect Rx K1 channel number
CSCwd26330	IMA3G does not generate FEBE's when BPV, P-bit, C-bit error are detected on the T3 port
CSCwc79322	Memory leak on ptpd_uea process
CSCwc76004	Wrong timestamp in TWAMP test packet with PTP active
CSCwd90840	mcast data traffic is getting dropped over vpls

Identifier	Headline
CSCwe27336	Error logs during reload in ASR920-24SZ-M variant
CSCwd28121	E1 loopback syslog and alarm reporting issues
CSCwd38074	Alarm reporting to IOS and L-bit propagation missing with STS1e-ct3-e1 mode
CSCwd48164	EVPN statd resource leak after protocol flaps
CSCwd44817	After router reload E1 framing gets changed to unframed in SDH VC12 mode with channe-group config
CSCwd11926	Need support for dual options in CLI for setting clock rate for x21
CSCwd16666	Only in 3GMS OC3 port with network loop Bert pattern is not syncing
CSCwd40951	CEM getting removed successfully even with wrong T1 number provided from same T3/E3
CSCwc77502	Unexpected reload due to MLDPv6
CSCwd67723	In IMA32D/IMA8D card, sometimes change in E1 controller config(after ctrlr flap)results in IM reboot
CSCwc84627	ASR-920-12SZ-IM goes continous reboot for a PCIE bus error
CSCwd78618	IMASER14A/S does not boot as expected.
CSCwd26357	rs485 with half-duplex configuration when reloaded, it gets into default full-duplex mode

Open Caveats – Cisco IOS XE Dublin 17.11.1a

Identifier	Headline
CSCwe42290	netconf intermittent connection issue due to checksum issue.
CSCwe34672	High CPU utilization on ptp_uea process
CSCwe54549	Unable to detect few SFPs.
CSCwe53791	EFP—Low throughput for rate step 900mbps+ when max-throughput command is disabled.
CSCwe38904	Frame loss seen for 64 bytes packet size for rate step 2333333/all kbps.

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