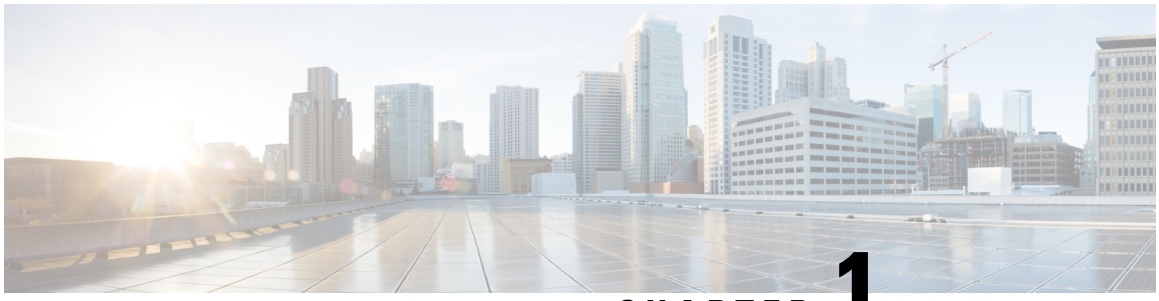
Release Notes for Cisco NCS 520 Series Ethernet Access Device, Cisco IOS XE Amsterdam 17.3.x

First Published: 2020-07-31

Last Modified: 2023-10-30

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.

Cisco NCS 520 Series Ethernet Access Device Overview

The Cisco NCS 520 Series Ethernet Access Device is a family of low cost, fixed Carrier Ethernet Network Interface Devices (NID) and a switch that is targeted to be the next generation replacement of the Cisco ME 3400 series Access Switches. The Cisco NCS 520 Series Ethernet Access Device adds 10G NID and low-cost MBH switch to the existing Service Provider Access portfolio, with the following features:

- MEF CE 3.0 compliant
- Premium SKUs with support for extended temperature (from -40C to 65C)
- Conformal coating on the PCBAs (to be able to support installation in ventilated enclosures)

This release note contains information about the Cisco NCS 520 Series Ethernet Access Device, provides features information for these devices, hardware support, limitations and restrictions, and caveats.

This release note provides information for these variants of the Cisco NCS 520 Series Ethernet Access Device:

- N520-4G4Z-A (Base)

- N520-X-4G4Z-A (Premium)
- N520-X-4G4Z-D (Premium)
- N520-20G4Z-A (Base)
- N520-20G4Z-D (Base)
- N520-X-20G4Z-A (Premium)
- N520-X-20G4Z-D (Premium)

Documentation Updates

Rearrangement in the Configuration Guides

- The following are the modifications in the CEM guides.
  - Introduction of the Alarm Configuring and Monitoring Guide:

    This guide provides the following information:
    - Alarms supported for SONET and SDH, and their maintenance
    - Alarm profiling feature
    - Auto In-Service States for cards, ports, and transceivers
  - Rearrangement of Chapter and Topics in the Alarm Configuring and Monitoring Guide:
    - The Auto In-Service States Guide is now a chapter inside the Alarms Configuring and Monitoring Guide.
    - Alarms at SONET Layers topic in the following CEM guides, is added to the Alarms Configuring and Monitoring Guide:
      - 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 Configuration Guide
    - The Alarm History and Alarm Profiling chapters are removed from the below CEM Technology guides, and added into the Alarm Configuring and Monitoring Guide:
      - 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 Configuration Guide

Limitations and Restrictions on the Cisco NCS 520 Series Ethernet Access Device

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.

- The **default interface** 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
  ```

- Adding or deleting the Trunk Ethernet flow points (TEFPs) with scaled bridge-domain, without delay causes the Cisco NCS 520 Series Ethernet Access Device to crash.
- Virtual services should be deactivated and uninstalled before performing replace operations.
- The **controller** and **nid-controller** commands are not supported.
- Cisco NCS 520 Series Ethernet Access Device displays an error in Hierarchical QoS policy while trying to remove the **bandwidth** and **bandwidth percent** commands from the default parent class dynamically. To remove the commands, you must first remove the bandwidth from child class and then from the parent class.
- When port is in OPER-DOWN state, applying Hierarchical QoS followed by speed change sets wrong bandwidth values on standard queues. To work around the mismatch, you must reattach the policy to the port level again.

Other Important Information

Upgrade to Cisco IOS XE 17.3.x

This section explains the procedure to upgrade the Cisco NCS 520 Series Ethernet Access Device from Cisco IOS XE Fuji 16.9.x and later to Cisco IOS XE Gibraltar 16.12.x and later.

The minimum base ROMMON version required to boot Cisco IOS XE Gibraltar 16.12.x and later release is **1.5**.

ROMMON version 1.5 is backward compatible. The backward compatibility of different ROMMON versions with IOS-XE versions are in the followig table:

Supported Cisco IOS-XE release	ROMMON Version
16.8.x 16.9.x 16.11.x	1.2
16.9.4 and later 16.11.2 and later 16.12.1 and later 17.1.1 and later	1.5
16.9.4 and later 16.11.2 16.12.1 and later 17.3.1 and later	1.6

Perform the following steps to migrate to Cisco IOS XE Amsterdam 17.3.x:

Step 1 On the command prompt, run the following command to check the current ROMMON version.

```
Device# show platform
Chassis type: N520-X-4G4Z-A
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      4xGE-4x10GE-FIXED   ok                    8w5d
R0        N520-X-4G4Z-A       ok, active            8w5d
F0                            ok, active            8w5d
P0        NCS520-PSU0         ok                    never
P1        NA                  ok                    never
P2        NCS520-FAN          ok                    never

Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
R0        0003001E            1.2(20180810:133528) [ncs520-dev] --> the ROMMON version is 1.2
F0        0003001E            1.2(20180810:133528) [ncs520-dev]
```

Note Do not migrate if the ROMMON version is 1.5 or above.

Step 2 Copy the running configuration to the bootflash for backup

```
Device# copy running-config bootflash:backup_config
Destination filename [backup_config]?
15549 bytes copied in 0.404 secs (38488 bytes/sec)
```

Step 3 Copy the migration image to bootflash location.

You can download the migration image from the location: https://software.cisco.com/download/home/286320761/type/286317642/release/1.5.

```
Device# copy tftp: bootflash:
Address or name of remote host []? 10.64.99.152
Source filename []? ncs520-1.5rommon-auto-upgrade-xe.bin
Destination filename [ncs520-1.5rommon-auto-upgrade-xe.bin]?
Accessing tftp://10.64.99.152/ ncs520-1.5rommon-auto-upgrade-xe.bin...
Loading ncs520-1.5rommon-auto-upgrade-xe.bin from 10.64.99.152 (via GigabitEthernet0):!!!
```

Step 4 Copy the Cisco IOS XE Amsterdam 17.3.x (or later) software image to bootflash.

Step 5 Set the boot variable to migration image and reload the router.

```
boot system bootflash:ncs520-1.5rommon-auto-upgrade-xe.bin
```

Caution Do not perform any power cycle or remove the power cable during the ROMMON upgrade. If there is a power loss during the upgrade, it may result in corruption of the boot image and it may require RMA of the equipment.

Step 6 Verify the ROMMON image version.

For RJ45 console: Look out for the following logs during bootup. These logs indicate successful ROMMON upgrade. After a successful ROMMON upgrade, the node auto reloads, which take at least five minutes.

```
Full Package address :0xC79BF018 Max-Address for IOS-Pkg Allocation:0xC79BEC18
%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Wed Jul 31 11:51:41 Universal 2019 PLEASE DO NOT POWER
 CYCLE ### BOOT LOADER UPGRADING

%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): Boot loader golden upgrade succesful


%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): Boot loader upgrade succesful
%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): To activate the new Rommon ,system will reload now!!!!

 %IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### After reload, PLEASE LOAD CCO IMAGE ###
N520-54-S1#show platform
Chassis type: N520-X-4G4Z-A

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      4xGE-4x10GE-FIXED   ok                    00:00:51
R0        N520-X-4G4Z-A       ok, active            00:03:07
F0                                       ok, active            00:03:07
P0        NCS520-PSU0         ok                    never
P1        NA                            ok                    never
P2        NCS520-FAN          ok                    never

Slot      CPLD Version        Firmware Version
--------- ------------------- ------------------------------------
R0        0003001E            1.5(20190415:181241) [ncs520-dev] --> the ROMMON version is 1.5
F0        0003001E            1.5(20190415:181241) [ncs520-dev]
```

For VTY Session: Wait for 30 minutes for auto upgrade to complete and the router to boot up. Reestablish the VTY session.

```
Device#show platform
Chassis type: N520-X-4G4Z-A

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      4xGE-4x10GE-FIXED   ok                    00:00:51
R0        N520-X-4G4Z-A       ok, active            00:03:07
F0                                       ok, active            00:03:07
P0        NCS520-PSU0         ok                    never
```

```
P1        NA                  ok                    never
P2        NCS520-FAN          ok                    never

Slot      CPLD Version        Firmware Version
--------- ------------------- ------------------------------------
R0        0003001E            1.5(20190415:181241) [ncs520-dev] --> the ROMMON version is 1.5
F0        0003001E            1.5(20190415:181241) [ncs520-dev]
```

Step 7 Set the boot variable to the Cisco IOS XE Amsterdam 17.3.x image and delete the migration image from the bootflash. Reload the router to activate the Cisco IOS XE Amsterdam 17.3.x software image.

```
Device#conf t

Device(config)#no boot system bootflash:ncs520-1.5rommon-auto-upgrade-xe.bin
Device(config)#boot system bootflash:<CCO Image>
Device(config)#end
Device#write memory
Device#del bootflash:ncs520-1.5rommon-auto-upgrade-xe.bin
```

Step 8 After booting the 17.3.x image, ROMMON and FPGA will automatically upgrade and the node will be reloaded. Once the node is up, the output will be:

```
Device#show platform
Chassis type: N520-X-20G4Z-A

Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0/0 20xGE-4x10GE-FIXED ok 1w5d
R0 N520-X-20G4Z-A ok, active 1w5d
F0 ok, active 1w5d
P0 NCS520-PSU0 ps, fail never
P1 NCS520-PSU1 ok never
P2 NCS520-FAN ok never

Slot CPLD Version Firmware Version
--------- ------------------- ------------------------------------
R0 00030025 1.6(20191125:124452) [ncs520-dev]
F0 00030025 1.6(20191125:124452) [ncs520-dev]
```

Software Licensing Overview

The Cisco NCS 520 Series Ethernet Access Device supports the following types of licenses:

- Port Licensing—Port Upgrade license is available as a "Pay as you Grow" model.
  - 10G upgrade license
  - 1G upgrade license
- Metro Access (default)

The following method is used to activate the above licenses:

- Cisco Software Licensing—The Cisco Software License Activation feature is a set of processes and components to activate Cisco software feature sets by obtaining and validating fee-based Cisco software licenses.

Note Licenses that are generated by the Cisco Software Licensing are tied to the UDI of the chassis and a corresponding watchtower device certificate (WDC) is stored in the system.

The following features are supported for the software licenses:

- QoS, with deep buffers and hierarchical QoS (HQOS)
- Layer 2: 802.1D, 802.1Q
- Ethernet Virtual Circuit (EVC)
- Ethernet OAM (802.11g, 802.3ah)
- IPv4 host connectivity
- IP Access License

Smart Licensing

If you are using Cisco IOS XE Bengaluru 17.6.1 or an earlier release version, Smart Licensing is not enabled by default. To enable Smart Licensing, see Software Activation Configuration Guide (Cisco NCS 520 Series).

Feature Navigator

Use the Cisco Feature Navigator to find information about feature, platform, and software image support. To access the Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on cisco.com is not required.

Supported Packages and System Requirements

Determining the Software Version

Use the following commands to verify your software version:

- Consolidated Package— **show version**

Supported FPGA Version

The table below lists the FPGA version of the software releases.

Table 1: FPGA Versions for this release

Release	FPGA Version
Cisco IOS XE Amsterdam 17.3.4	0x00030025

Cisco IOS XE Amsterdam 17.3.5	0x00030025
Cisco IOS XE Amsterdam 17.3.6	0x00030025
Cisco IOS XE Amsterdam 17.3.7	0x00030025
Cisco IOS XE Amsterdam 17.3.8	0x00030025
Cisco IOS XE Amsterdam 17.3.8a	0x00030025

Note FPGA will automatically upgrade to **0x00030025** from Cisco IOS XE Amsterdam 17.3.x onwards.

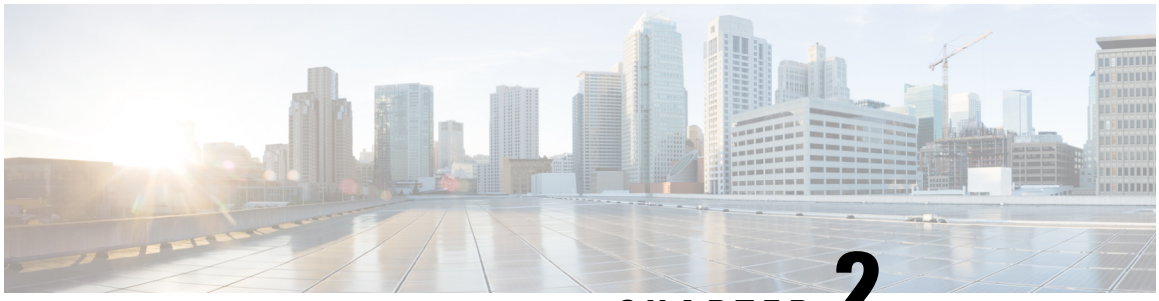
The Cisco NCS 520 Series Ethernet Access Device will take around 210 seconds to reboot after a successful FPGA upgrade. Do not power-cycle the Ethernet Access Device during FPGA upgrade.

Supported ROMMON Version

Table 2: Supported ROMMON Version

Supported Cisco IOS-XE Release	ROMMON Version
Cisco IOS XE Amsterdam 17.3.4	1.6
Cisco IOS XE Amsterdam 17.3.5	1.6
Cisco IOS XE Amsterdam 17.3.6	1.6
Cisco IOS XE Amsterdam 17.3.7	1.6
Cisco IOS XE Amsterdam 17.3.8	1.6
Cisco IOS XE Amsterdam 17.3.8a	1.6

Note ROMMON will automatically upgrade to **1.6** from Cisco IOS XE Amsterdam 17.3.x onwards.



CHAPTER 2

What's New for Cisco IOS XE Amsterdam 17.3.x

This chapter describes the new hardware and software features supported on the Cisco NCS 520 Series Ethernet Devices in Cisco IOS XE Amsterdam 17.3.x.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.8a

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.8a

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 Amsterdam 17.3.8

There are no new Hardware features introduced for this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.8

There are no new Software features introduced for this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.7

There are no new Software features introduced for this release.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.7

There are no new Hardware features introduced for this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.6

There are no new Software features introduced for this release.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.6

There are no new Hardware features introduced for this release.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.5

There are no new Hardware features introduced for this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.5

There are no new Software features introduced for this release.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.4

There are no new Hardware features introduced for this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.4

There are no new Hardware features introduced for this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.3

There are no new Software features introduced for this release.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.3

There are no new Hardware features introduced for this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.2a

There are no new Software features introduced for this release.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.2a

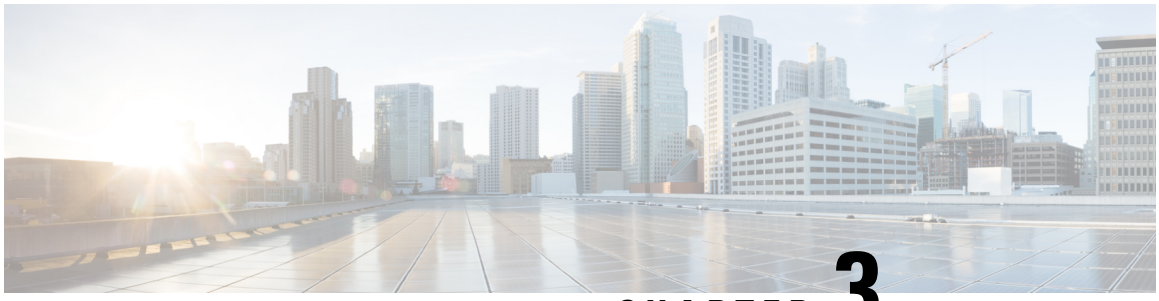
There are no new Hardware features introduced for this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.1

Feature	Description
IP Addressing	
DHCP Snooping	The Dynamic Host Configuration Protocol (DHCP) Snooping is a DHCP security feature that provides network securityby filtering untrusted DHCP messages and by building and maintaining a DHCP Snooping binding database, DHCP snooping acts like a firewall between untrusted hosts and DHCP servers.DHCP Snooping is used to differentiate untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another router. This feature is supported on the Cisco NCS 520 Router.
Dynamic ARP Inspection	The dynamic Address Resolution Protocol (ARP) provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. Dynamic ARP inspection also determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, such as the DHCP Snooping binding database. This feature is supported on the Cisco NCS 520 Router.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.1

There are no new Hardware features introduced for 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.

Open Caveats – Cisco IOS XE Amsterdam 17.3.8a

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.8a

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

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.8

There are no resolved caveats for this release.

Open Caveats – Cisco IOS XE Amsterdam 17.3.8

Identifier	Headline
CSCwe84096	Router unable to reload due to `periodic.sh` process.

Open Caveats – Cisco IOS XE Amsterdam 17.3.7

There are no open caveats for this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.7

There are no resolved caveats for this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.6

Identifier	Headline
CSCwc38933	NCS520 change "no negotiation auto" to "negotiation auto" after multiple power cycles

Open Caveats – Cisco IOS XE Amsterdam 17.3.6

There are no open caveats for this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.5

Identifier	Headline
CSCvy29440	Egress Service Policy Removed from Interface on Reload

Open Caveats – Cisco IOS XE Amsterdam 17.3.5

There are no open caveats for this release.

Open Caveats – Cisco IOS XE Amsterdam 17.3.4

Caveat ID Number	Description
CSCvy29440	Egress Service Policy Removed from Interface on Reload

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.4

Caveat ID Number	Description
CSCvx08157	Communication problem with newly added BDI when remove some BDI before

Open Caveats – Cisco IOS XE Amsterdam 17.3.3

There are no open caveats for this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
CSCvw56579	Malformed IPv6 frame generated Randomly
CSCvw66719	Bridge Domain Routing does not work after interface flap

Open Caveats – Cisco IOS XE Amsterdam 17.3.2a

There are no Open caveats for this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.2a

Caveat ID Number	Description
CSCvw13768	Route-map CLI not visible in latest images

Open Caveats – Cisco IOS XE Amsterdam 17.3.1

There are no Open caveats for this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.1

Caveat ID Number	Description
CSCvs18938	DMM reports a very high delay and jitter values periodically
CSCvs73046	Adding new VLAN, causes traffic loop in REP ring
CSCvs76696	After restart NCS520 smart license registration will fail
CSCvt91240	ZTP changes to give precedence to untagged BDI
CSCvu27592	Enable 10G port during ZTP without license.

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