

Release Notes for Cisco NCS 520 Series Ethernet Access Device, 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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Cisco NCS 520 Series Ethernet Access Device Overview** 1

Feature Navigator 2

Feature Matrix 2

Software Licensing Overview 2

Upgrade to Cisco IOS XE Dublin 17.11.x 3

Supported Packages and System Requirements 6

Supported FPGA Version 6

Supported ROMMON Version 6

Limitations and Restrictions on the Cisco NCS 520 Series Ethernet Access Device 7

CHAPTER 2 **What's New for Cisco IOS XE Dublin 17.11.x** 9

What's New in Software for Cisco IOS XE Dublin 17.11.1a 9

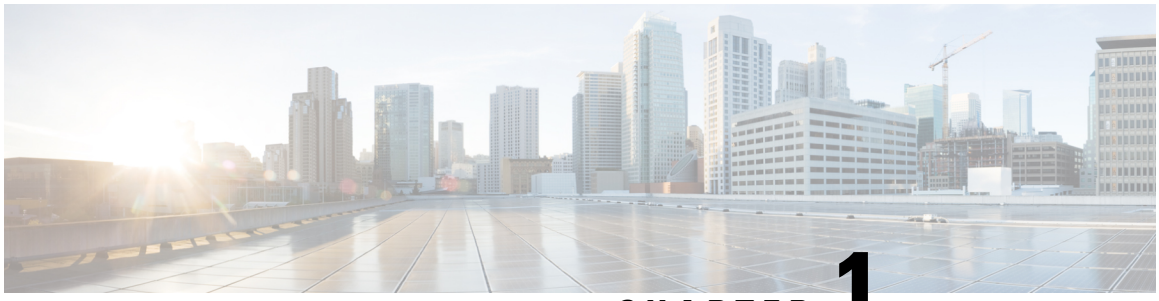
What's New in Hardware for Cisco IOS XE Dublin 17.11.1a 9

CHAPTER 3 **Caveats** 11

Resolved Caveats – Cisco IOS XE Dublin 17.11.1a 11

Open Caveats – Cisco IOS XE Dublin 17.11.1 11

Cisco Bug Search Tool 12



CHAPTER 1

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)

- Feature Navigator, on page 2
- Feature Matrix, on page 2
- Software Licensing Overview, on page 2
- Upgrade to Cisco IOS XE Dublin 17.11.x, on page 3
- Supported Packages and System Requirements, on page 6
- Limitations and Restrictions on the Cisco NCS 520 Series Ethernet Access Device, on page 7

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.

Feature Matrix

The feature matrix lists the features supported for each platform. For more information, see the Cisco NCS 520 Ethernet Access Devices Feature Compatibility Matrix.

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).

Upgrade to Cisco IOS XE Dublin 17.11.x

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

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

Supported Cisco IOS XE release	Supported ROMMON Version
Cisco IOS XE Fuji 16.8.x Cisco IOS XE Fuji 16.9.x Cisco IOS XE Gibraltar 16.11.x	1.2
Cisco IOS XE Fuji 16.9.4 and later Cisco IOS XE Gibraltar 16.11.2 and later Cisco IOS XE Gibraltar 16.12.1 and later Cisco IOS XE Amsterdam 17.1.1 and later	1.5
Cisco IOS XE Amsterdam 17.3.1 and later Cisco IOS XE Bengaluru 17.4.1 and later Cisco IOS XE Bengaluru 17.5.1 and later Cisco IOS XE Bengaluru 17.6.x and later Cisco IOS XE Cupertino 17.7.x and later Cisco IOS XE Cupertino 17.8.x and later Cisco IOS XE Cupertino 17.9.x and later Cisco IOS XE Dublin 17.10.x and later Cisco IOS XE Dublin 17.11.x and later	1.6 **Note** The Cisco IOS XE versions that support ROMMON version 1.5, are also supported for 1.6.

Perform the following steps to migrate to Cisco IOS XE Dublin 17.11.x:

SUMMARY STEPS

1. At the command prompt, run the following command to check the current ROMMON version.
2. Copy the running configuration to the bootflash for backup.
3. Copy the migration image to a bootflash location.
4. Copy the Cisco IOS XE Dublin 17.11.x software image to bootflash.
5. Set the boot variable to migration image and reload the router.
6. Verify the ROMMON image version.

7. Set the boot variable to the Cisco IOS XE Dublin 17.11.x software image and delete the migration image from the bootflash. Reload the router to activate the Cisco IOS XE Dublin 17.10.x software image.
8. After booting the Cisco IOS XE Dublin 17.11.x image, ROMMON and FPGA will automatically upgrade and the node is reloaded. Once the node is up, the output is displayed:

DETAILED STEPS

Procedure

Step 1 At 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 a 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 Dublin 17.11.x 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 the RJ-45 console: Check for the following logs during bootup. These logs indicate successful ROMMON upgrade. After a successful ROMMON upgrade, the node auto reloads. This action takes at least 5 minutes to complete successfully.

```
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 Dublin 17.11.x software image and delete the migration image from the bootflash. Reload the router to activate the Cisco IOS XE Dublin 17.10.x software image.

```
Device#configure terminal
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 Cisco IOS XE Dublin 17.11.x image, ROMMON and FPGA will automatically upgrade and the node is reloaded. Once the node is up, the output is displayed:

```
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]
```

Supported Packages and System Requirements

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 Dublin 17.11.1a	0x00030025

Note The FPGA automatically upgrades to **0x00030025** from Cisco IOS XE Cupertino 17.7.1 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 Dublin 17.11.1	1.6

Note ROMMON automatically upgrades to **1.6** from Cisco IOS XE Cupertino 17.7.1 onwards.

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.

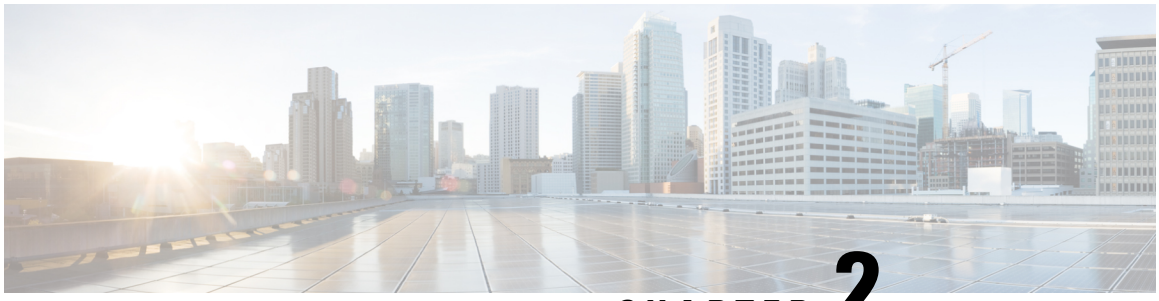
We recommend performing a reload of the router. As a result, above alarm will not be seen during the next reload due to FSCK(file systems check) execution.

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.



CHAPTER 2

What's New for Cisco IOS XE Dublin 17.11.x

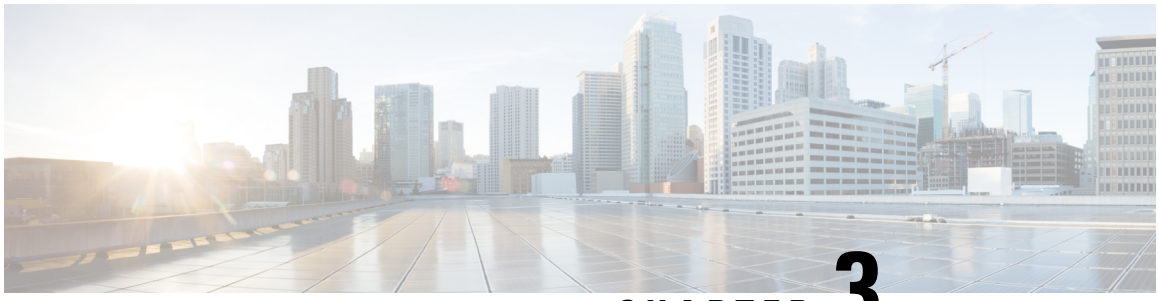
- What's New in Software for Cisco IOS XE Dublin 17.11.1a, on page 9
- What's New in Hardware for Cisco IOS XE Dublin 17.11.1a, on page 9

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

Feature	Description
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.

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

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.

- Resolved Caveats – Cisco IOS XE Dublin 17.11.1a, on page 11
- Open Caveats – Cisco IOS XE Dublin 17.11.1, on page 11
- Cisco Bug Search Tool, on page 12

Resolved Caveats – Cisco IOS XE Dublin 17.11.1a

Identifier	Headline
CSCwc56918	NCS520: IPv6 host functionality config fails after upgrade to latest image
CSCwe07340	Static route not programmed in CEF when more than six static routes use the same next hop ip address
CSCwb68238	CSPN SSH requirement

Open Caveats – Cisco IOS XE Dublin 17.11.1

Identifier	Headline
CSCwe53050	Misreporting Output Drops as Errors in Interface counters

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