



Release Notes for Cisco NCS 4206 and Cisco NCS 4216 Series, Cisco IOS XE Dublin 17.11.x

First Published: 2023-04-07

Last Modified: 2023-04-06

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 NON-INFRINGEMENT 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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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

Introduction 1

| | |
|---|----|
| Overview of Cisco NCS 4206 and NCS 4216 | 1 |
| Cisco NCS 4206 | 1 |
| Cisco NCS 4216 | 2 |
| NCS 4216 14RU | 2 |
| Feature Navigator | 2 |
| Hardware Supported | 3 |
| Cisco NCS 4206 Supported Interface Modules | 3 |
| Supported Interface Modules | 3 |
| Cisco NCS 4216 Supported Interface Modules | 5 |
| Cisco NCS 4216 F2B Supported Interface Modules | 5 |
| Restrictions and Limitations | 5 |
| Determining the Software Version | 8 |
| Upgrading to a New Software Release | 8 |
| Supported FPGA Versions for NCS 4206 and NCS 4216 | 9 |
| Additional References | 12 |

CHAPTER 2

What's New for Cisco IOS XE Dublin 17.11.x 15

| | |
|---|----|
| What's New in Hardware for Cisco IOS XE Dublin 17.11.1a | 15 |
| What's New in Software for Cisco IOS XE Dublin 17.11.1a | 15 |

CHAPTER 3

Caveats 19

| | |
|---|----|
| Resolved Caveats - Cisco IOS XE Dublin 17.11.1a | 19 |
| Open Caveats - Cisco IOS XE Dublin 17.11.1a | 20 |
| Cisco Bug Search Tool | 21 |



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 4206 and Cisco NCS 4216 beginning with Cisco IOS XE Release 3.18SP.

- [Overview of Cisco NCS 4206 and NCS 4216, on page 1](#)
- [Feature Navigator, on page 2](#)
- [Hardware Supported, on page 3](#)
- [Restrictions and Limitations, on page 5](#)
- [Determining the Software Version, on page 8](#)
- [Upgrading to a New Software Release, on page 8](#)
- [Supported FPGA Versions for NCS 4206 and NCS 4216, on page 9](#)
- [Additional References, on page 12](#)

Overview of Cisco NCS 4206 and NCS 4216

Cisco NCS 4206

The Cisco NCS 4206 is a fully-featured aggregation platform designed for the cost-effective delivery of converged mobile and business services. With shallow depth, low power consumption, and an extended temperature range, this compact 3-rack-unit (RU) chassis provides high service scale, full redundancy, and flexible hardware configuration.

The Cisco NCS 4206 expands the Cisco service provider product portfolio by providing a rich and scalable feature set of Layer 2 VPN (L2VPN) and Layer 3 VPN (L3VPN) services in a compact package. It also supports a variety of software features, including Carrier Ethernet features, Timing over Packet, and pseudowire.

For more information on the Cisco NCS 4206 Chassis, see the [Cisco NCS 4206 Hardware Installation Guide](#).

Cisco NCS 4216

The Cisco NCS 4216 is a seven-rack (7RU) unit chassis that belongs to the Cisco NCS 4200 family of chassis. This chassis complements Cisco's offerings for IP RAN solutions for the GSM, UMTS, LTE and CDMA. Given its form-factor, interface types and Gigabit Ethernet density the Cisco NCS 4216 can also be positioned as a Carrier Ethernet aggregation platform.

The Cisco NCS 4216 is a cost optimized, fully redundant, centralized forwarding, extended temperature, and flexible pre-aggregation chassis.

For more information about the Cisco NCS 4216 Chassis, see the [Cisco NCS 4216 Hardware Installation Guide](#).

Cisco NCS 4216 F2B

The Cisco NCS 4216 F2B is a 14-rack unit router that belongs to the Cisco NCS 4200 family of routers. This router complements Cisco's offerings for IP RAN solutions for the GSM, UMTS, LTE, and CDMA. Given its form-factor, interface types, and Gigabit Ethernet density the Cisco NCS 4216 F2B can also be positioned as a Carrier Ethernet aggregation platform.

The Cisco NCS 4216 F2B is a cost optimized, fully redundant, centralized forwarding, extended temperature, and flexible pre-aggregation router.

For more information about the Cisco NCS 4216 F2B Chassis, see the [Cisco NCS 4216 F2B Hardware Installation Guide](#).

NCS 4216 14RU

The Cisco NCS 4216 14RU is a 14-rack unit router that belongs to the Cisco NCS 4200 family of routers. This router complements Cisco's offerings for IP RAN solutions for the GSM, UMTS, LTE, and CDMA. Given its form-factor, interface types and Gigabit Ethernet density the Cisco NCS 4216 14RU can also be positioned as a Carrier Ethernet aggregation platform.

The Cisco NCS 4216 14RU is a cost optimized, fully redundant, centralized forwarding, extended temperature, and flexible pre-aggregation router.

For more information about the Cisco NCS 4216 14RU chassis, see the [Cisco NCS 4216 14RU 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

The following sections list the hardware supported for Cisco NCS 4206 and Cisco NCS 4216 chassis.

Cisco NCS 4206 Supported Interface Modules

Supported Interface Modules



Note If the **license feature service-offload enable** command is configured, then the NCS4200-1T8LR-PS IM is not supported in the router for RSP3.



Note There are certain restrictions in using the interface modules on different slots in the chassis. Contact Cisco Sales/Support for the valid combinations.



Note FAN OIR is applicable every time the IM based fan speed profile is switched to NCS4200-1H-PK= and NCS4200-2Q-P interface modules. Even though the IMs remain in the Out-of-Service state, they are still considered as present in the chassis.

Table 1: NCS420X-RSP Supported Interface Modules and Part Numbers

| RSP Module | Supported Interface Modules | Part Numbers | Slot |
|-------------|--|-------------------|---------------------------|
| NCS420X-RSP | 8-port 10 Gigabit Ethernet Interface Module (8X10GE) | NCS4200-8T-PS | All |
| | 1-port 100 Gigabit Ethernet Interface Module (1X100GE) | NCS4200-1H-PK= | 4 and 5 |
| | 2-port 40 Gigabit Ethernet QSFP Interface Module (2X40GE) | NCS4200-2Q-P | 4 and 5 |
| | 8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module | NCS4200-1T16G-PS | 0,3,4, and 5 |
| | 1-port OC-192 Interface module or 8-port Low Rate Interface Module | NCS4200-1T8S-10CS | 2,3,4, and 5 |
| | NCS 4200 1-Port OC-192 or 8-Port Low Rate CEM 20G Bandwidth Interface Module | NCS4200-1T8S-20CS | 2,3,4, and 5 ¹ |
| | 48-port T1/E1 CEM Interface Module | NCS4200-48T1E1-CE | All |
| | 48-port T3/E3 CEM Interface Module | NCS4200-48T3E3-CE | All |
| | 2-port 100 Gigabit Ethernet (QSFP) Interface Module (2X100GE) ² | NCS4200-2H-PQ | 4,5 |
| | 1-port OC48 ³ / STM-16 or 4-port OC-12/OC-3 / STM-1/STM-4 + 12-port T1/E1 + 4-Port T3/E3 CEM Interface Module | NCS4200-3GMS | 2,3,4, and 5 |

¹ These slots are supported on 10G or 20G mode.

² IM supports only one port of 100G with RSP3 as QSFP28 on Port 0 in both slots 4 and 5.

³ If OC48 is enabled, then the remaining 3 ports are disabled.

Table 2: NCS420X-RSP-128 Supported Interface Modules and Part Numbers

| RSP Module | Supported Interface Modules | Part Numbers | Slot |
|-------------|--|------------------|--------------|
| NCS420X-RSP | SFP Combo IM—8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet Interface Module (1X10GE) | NCS4200-1T8LR-PS | All |
| | 8-port T1/E1 CEM Interface Module | NCS4200-8E1T1-CE | All |
| | 1-port OC48 ⁴ / STM-16 or 4-port OC-12/OC-3 / STM-1/STM-4 + 12-port T1/E1 + 4-Port T3/E3 CEM Interface Module | NCS4200-3GMS | 2,3,4, and 5 |

⁴ If OC48 is enabled, then the remaining 3 ports are disabled.

Cisco NCS 4216 Supported Interface Modules

For information on supported interface modules, see [Supported Interface Modules](#).

Cisco NCS 4216 F2B Supported Interface Modules

For information on supported interface modules, see [Supported Interface Modules](#).

Restrictions and Limitations



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 ASR 900NCS 4200 routers.
- From the Cisco IOS XE 16.6.1 releases, In-Service Software Upgrade (ISSU) is not supported on the router to the latest releases. For more information on the compatible release versions, see [ISSU Support Matrix](#).
- ISSU is not supported between a Cisco IOS XE 3S release and the Cisco IOS XE Bengaluru 17.6.x release.
- The port restriction on 1-port OC-192 or 8-port low rate CEM interface module is on port pair groups. If you have OC48 configured on a port, the possible port pair groups are 0–1, 2–3, 4–5, 6–7. If one of the ports within this port group is configured with OC48 rate, the other port cannot be used.
- RS422 pinout works only on ports 0–7.
- The **ip cef accounting** command is *not* supported on the router.
- Configuration sync does *not* happen on the Standby RSP when the active RSP has Cisco Software Licensing configured, and the standby RSP has Smart Licensing configured on the router. If the active RSP has Smart Licensing configured, the state of the standby RSP is undetermined. The state could be pending or authorized as the sync between the RSP modules is not performed.
- Evaluation mode feature licenses may not be available to use after disabling, and enabling the smart licensing on the RSP2 module. A reload of the router is required.

- Ingress counters are not incremented for packets of the below format on the RSP3 module for the 10-Gigabit Ethernet interfaces, 100-Gigabit Ethernet interfaces, and 40-Gigabit Ethernet interfaces:

Packet Format

MAC header---->VLAN header---->Length/Type

When these packets are received on the RSP3 module, the packets are not dropped, but the counters are not incremented.

- T1 SAToP, T3 SAToP, and CT3 are supported on an UPSR ring only with local connect mode. Cross-connect configuration of T1, T3, and CT3 circuits to UPSR are not supported.
- PTP is not supported when 8-port 10-Gigabit Ethernet interface module is in oversubscribed mode.
- Port channel 61–64 is not supported in the 16.11.1a release. The range of configurable port channel interfaces has been limited to 60.
- Effective with Cisco IOS XE Everest 16.6.1, the VPLS over Port-channel (PoCH) scale is reduced from 48 to 24 for Cisco ASR 903 RSP3 module.



Note The PoCH scale for Cisco ASR 907 routers is 48.

- The frame drops may occur for packets with packet size of less than 100 bytes, when there is a line rate of traffic over all 1G or 10G interfaces available in the system. This restriction is applicable only on RSP2 module, and is not applicable for RSP3 module.
- One Ternary Content-Addressable Memory (TCAM) entry is utilized for Segment Routing Performance Measurement. This is required for the hardware timestamping to function.
- 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 during the auto upgrade. However, the router can be reloaded during the next planned reload to complete the secondary ROMMON upgrade. This is applicable to ASR 903 and ASR 907 routers.
- In the Cisco IOS XE 17.1.1 release, the EVPN EVI type is VLAN-based by default, and while configuring for the EVPN EVI type, it is recommended to configure the EVPN EVI type as VLAN-based, VLAN bundle and VLAN aware model.
- For Cisco IOS XE Gibraltar Release 16.9.5, Cisco IOS XE Gibraltar Release 16.12.3, and Cisco IOS XE Amsterdam 17.1.x, a minimum disk space of 2 MB is required in the boot flash memory file system for a successful ROMMON auto upgrade process. For a disk space lesser than 2 MB, ROMMON auto upgrade fails and the router reboots. This is applicable to Cisco ASR 903 and Cisco ASR 907 routers.
- In the Cisco IOS XE 16.12.1, 17.1.1, and 17.2.1 releases, IPsec is not supported on the Cisco RSP3 module.
- CEM circuit provisioning issues may occur during downgrade from Cisco IOS XE Amsterdam 17.3.1 to any lower versions or during upgrade to Cisco IOS XE Amsterdam 17.3.1 from any lower versions, if the CEM scale values are greater than 10500 APS/UPSR in protected CEM circuits. So, ensure that the CEM scale values are not greater than 10500, during ISSU to or from 17.3.1.
- Some router models are not fully compliant with all IETF guidelines as exemplified by running the pyang tool with the **lint** flag. The errors and warnings that are exhibited by running the pyang tool with the **lint** flag are currently noncritical as they do not impact the semantic of the models or prevent the models

from being used as part of the toolchains. A script has been provided, "check-models.sh", that runs pyang with **lint** validation enabled, but ignoring certain errors. This allows the developer to determine what issues may be present.

As part of model validation for the Cisco IOS XE Amsterdam 17.3.1 release, "LEAFREF_IDENTIFIER_NOT_FOUND" and "STRICT_XPATH_FUNCTIONS" error types are ignored.

- Test Access Port (TAP) is not supported when the iMSG VLAN handoff feature is enabled on the same node.
- Data Communication Channel (DCC) is not supported in the A900-IMA1Z8S-CXMSNCS4200-1T8S-20CS interface module for the Cisco IOS XE Cupertino 17.8.1 release.
- In RSP2 and RSP3 modules, during In-Service Software Upgrade (ISSU), interface modules undergo FPGA upgrade.

The following table details the IM Cisco IOS XE versions during ISSU with respect to FPGA upgrade and the impact of traffic flow for these IMs:

Table 3: Impact on IM during ISSU and FPGA Upgrade

| IM | IM Version During ISSU | Pre-ISSU FPGA Upgrade | Post-ISSU Impact on IM | FPGA Version post ISSU |
|----------------|---|--|-------------------------------------|---|
| Phase 1 | Cisco IOS XE 17.3.x or earlier version to Cisco IOS XE 17.4.x | FPGA upgrade completes and IM starts after the reload process. FPGA version (phase -1) - 0.47 | Traffic is impacted during upgrade. | 0.75 |
| Phases 1 and 2 | Version earlier to Cisco IOS XE 17.8.x | FPGA upgrade completes and IM starts after the reload process. <ul style="list-style-type: none"> • FPGA version (Phase 1)—0.47 • FPGA version (Phase 2) <ul style="list-style-type: none"> • AMA1Z-02 • NS101S-02 • Combo IM: 69.24 | Traffic is impacted during upgrade. | <ul style="list-style-type: none"> • FPGA version (Phase 1)—0.75 • FPGA version (Phase 2) <ul style="list-style-type: none"> • AMA1Z-02 • NS101S-02 • Combo IM: 69.32 |

| IM | IM Version During ISSU | Pre-ISSU FPGA Upgrade | Post-ISSU Impact on IM | FPGA Version post ISSU |
|---------|--|--|--------------------------|------------------------|
| Phase 1 | Cisco IOS XE 17.4.1 or later versions to Cisco IOS XE 17.8.1 | IM FPGA already upgraded with the latest version and reload is not required. | Traffic is not impacted. | 0.75 |

For more information on the FPGA versions, see [Supported FPGA, HoFPGA, and ROMMON VersionsSupported FPGA Versions](#).

Refer the following table for supported IMs:

Table 4: ASR 900 Supported Ethernet Interface Module

| Phase 1 IM | Phase 2 IM | Phase 3 IM |
|-------------|--------------|------------|
| A900-IMA8S | A900-IMA8S1Z | A900-IMA8Z |
| A900 -IMA8T | A900-IMA8T1Z | A900-IMA2F |
| A900-IMA1X | A900-IMA2Z | A900-IMA2C |

Table 5: NCS 4200 Supported Ethernet Interface Module

| Phase 1 IM | Phase 2 IM | Phase 3 IM |
|---------------|------------------|---------------|
| NCS4200-1T8LR | NCS4200-1T8LR-PS | NCS4200-8T-PS |
| | | NCS4200-2Q-P |
| | | NCS4200-2H-PQ |

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)

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 ASR 900 Series Routers](#) [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 on 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 firmware upgrade.

ROMMON Version

We recommend you to upgrade the ROMMON version to 15.6(49r)S.

For more information on the ROMMON package, see [Cisco Software Download](#).



Note ROMMON upgrade is mandatory to boot RSP3 images.

Supported FPGA Versions for NCS 4206 and NCS 4216

Use the **show hw-module all fpd** command to display the IM FPGA version on the chassis.

Use the **show platform software agent iomd [slot/subslot] firmware cem-fpga** command to display the CEM FPGA version on the chassis.

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



Note During ISSU, TDM interface modules are reset for FPGA upgrade.

Table 6: Supported TDM IM and CEM FGAs for NCS 4206-RSP3 and NCS 4216

| Category | Cisco IOS XE Release | 48 X T1/E1 CEM Interface Module FPGA | 48 X T3/E3 CEM Interface Module FPGA | OC-192 Interface Module + 8-port Low Rate Interface Module FPGA | NCS 4200-1T8S-20CS | NCS4200-3GMS |
|----------|----------------------|--------------------------------------|--------------------------------------|---|--------------------------------------|--------------|
| IM FPGA | 17.11.1a | 1.22 | 1.22 | 1.15 | 0.95 | 2.0 |
| CEM FPGA | | 7.0 | 5.6 | 5G mode: 6.5 10G mode: 7.9 | 10G mode: 7.4 20G mode: 7.5 | 9.3 |

| Category | Cisco IOS XE Release | 48 X T1/E1 CEM Interface Module FPGA | 48 X T3/E3 CEM Interface Module FPGA | OC-192 Interface Module + 8-port Low Rate Interface Module FPGA | NCS 4200-1T8S-20CS | NCS4200-3GMS |
|----------|----------------------|--------------------------------------|--------------------------------------|---|--|--------------|
| IM FPGA | 17.10.1 | 1.22 | 1.22 | 1.15 | 0.95 | 2.0 |
| CEM FPGA | | 6.0 | 5.2 | 5G mode: 6.5 10G mode: 7.9 | 10G mode: 7.3 20G mode: 7.3 | 9.3 |
| IM FPGA | 17.9.2 | 1.22 | 1.22 | 1.15 | 0.95 | 2.0 |
| CEM FPGA | | 6.0 | 5.2 | 5G mode: 6.5 10G mode: 7.9 | 10G mode: 7.2 20G mode: 7.2 | 9.1 |
| IM FPGA | 17.9.1 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 |
| CEM FPGA | | 6.0 | 5.2 | 5G mode: 6.5 10G mode: 7.9 | 10G mode: 7.2 20G mode: 7.2 | 9.1 |
| IM FPGA | 17.8.1 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 |
| CEM FPGA | | 6 | 5.2 | 5G mode: 6.5 10G mode: 7.9 | 10G mode: 7.0 20G mode: 6.0 | 9.0 |
| IM FPGA | 17.7.1 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 |
| CEM FPGA | | 0x52110052 | 0x52520052 | 5G mode: 0x10090065 10G mode: 0x10070079 | 10G mode: 0x10290051 20G mode: 0x10290051 | 0x10030076 |

| Category | Cisco IOS XE Release | 48 X T1/E1 CEM Interface Module FPGA | 48 X T3/E3 CEM Interface Module FPGA | OC-192 Interface Module + 8-port Low Rate Interface Module FPGA | NCS 4200-1T8S-20CS | NCS4200-3GMS |
|----------|----------------------|--------------------------------------|--------------------------------------|---|--|--------------|
| IM FPGA | 17.6.2 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 |
| CEM FPGA | | 0x52110052 | 0x52520052 | 5G mode: 0x10090065 10G mode: 0x10070079 | 10G mode: 0x10290051 20G mode: 0x10290051 | 0x10030076 |
| IM FPGA | 17.6.1 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 |
| CEM FPGA | | 0x52110052 | 0x52520052 | 5G mode: 0x10090065 10G mode: 0x10070079 | 10G mode: 0x10290051 20G mode: 0x10290051 | 0x10030076 |
| IM FPGA | 17.5.1 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 |
| CEM FPGA | | 0x52050052 | 0x52420052 | 5G mode: 0x10210063 10G mode: 0x10530078 | 10G mode: 0x10090051 20G mode: 0x10090051 | 0x10020076 |

Table 7: Supported Ethernet IM FPGA/FPD versions for NCS 4206-RSP3 and NCS 4216

| Cisco IOS XE Release | NCS4200-1T16G-PS | NCS4200-1T8LR-PS | NCS4200-8T-PS | NCS4200-2Q-P | NCS4200-1H-PK | NCS4200-2H-PQ | NCS4200-1T16LR |
|----------------------|------------------|------------------|---------------|--------------|---------------|---------------|----------------|
| 17.11.1a | 1.129 | 69.32 | 0.21 | 0.21 | 0.20 | 0.20 | 69.24 |
| 17.10.1 | 1.129 | 69.32 | 0.21 | 0.21 | 0.20 | 0.20 | 69.24 |
| 17.10.1 | 1.129 | 69.32 | 0.21 | 0.21 | 0.20 | 0.20 | 69.24 |
| 17.9.2 | 1.129 | 69.32 | 0.21 | 0.21 | 0.22 | 0.20 | 69.24 |
| 17.9.1 | 1.129 | 69.32 | 0.21 | 0.21 | 0.22 | 0.20 | 69.24 |
| 17.8.1 | 1.129 | 69.32 | 0.21 | 0.21 | 0.22 | 0.20 | 69.24 |
| 17.7.1 | 1.129 | 1.129 | 0.21 | 0.21 | 0.22 | 0.20 | 69.24 |
| 17.6.1 | 1.129 | 1.129 | 0.21 | 0.21 | 0.22 | 0.20 | 69.24 |
| 17.5.1 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 | 0.23 | 0.20 |
| 17.4.1 | 1.129 | 69.24 | 0.21 | 0.22 | 0.20 | 3.4 | 1.129 |

Table 8: FPGA, HoFPGA, and ROMMON Versions for Cisco IOS XE 17.11.1 Release

| Platform | Interface Module | FPGA Current Version | FPGA Minimum Required Version | RSP HoFPGA Active | RSP HoFPGA Standby | ROMMON |
|-----------------|------------------|----------------------|-------------------------------|-------------------|--------------------|------------|
| NCS420X-RSP-128 | NCS4200-1T8LR-PS | 0.75 | 0.75 | 0X00030011 | 0X00030011 | 15.6(54r)S |
| NCS4206-RSP | NCS4200-1H-PK | 0.20 | 0.20 | 40035 | 40035 | 15.6(57r)S |
| | NCS4200-8T-PS | 0.22 | 0.21 | | | |
| | NCS4200-1T8LR-PS | 69.32 | 69.32 | | | |
| NCS4216-RSP | NCS4200-1H-PK | 0.20 | 0.20 | 20040034 | 20040034 | 15.6(57r)S |

Additional References

Deferrals

Cisco IOS software images are subject to deferral. We recommend that you view the deferral notices at the following location to determine whether your software release is affected:

http://www.cisco.com/en/US/products/products_security_advisories_listing.html.

Field Notices and Bulletins

- Field Notices—We recommend that you view the field notices for this release to determine whether your software or hardware platforms are affected. You can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

MIB Support

The below table summarizes the supported MIBs on the Cisco NCS 4206 and Cisco NCS 4216.

| Supported MIBs | | |
|---------------------------------|---|---------------------------------|
| BGP4-MIB (RFC 1657) | CISCO-IMAGE-LICENSE-MGMT-MIB | MPLS-LDP-STD-MIB (RFC 3815) |
| CISCO-BGP-POLICY-ACCOUNTING-MIB | CISCO-IMAGE-MIB | MPLS-LSR-STD-MIB (RFC 3813) |
| CISCO-BGP4-MIB | CISCO-IPMROUTE-MIB | MPLS-TP-MIB |
| CISCO-BULK-FILE-MIB | CISCO-LICENSE-MGMT-MIB | MSDP-MIB |
| CISCO-CBP-TARGET-MIB | CISCO-MVPN-MIB | NOTIFICATION-LOG-MIB (RFC 3014) |
| CISCO-CDP-MIB | CISCO-NETSYNC-MIB | OSPF-MIB (RFC 1850) |
| CISCO-CEF-MIB | CISCO-OSPF-MIB (draft-ietf-ospf-mib-update-05) | OSPF-TRAP-MIB (RFC 1850) |

| Supported MIBs | | |
|---------------------------------|--|------------------------------------|
| CISCO-CLASS-BASED-QOS-MIB | CISCO-OSPF-TRAP-MIB (draft-ietf-ospf-mib-update-05) | PIM-MIB (RFC 2934) |
| CISCO-CONFIG-COPY-MIB | CISCO-PIM-MIB | RFC1213-MIB |
| CISCO-CONFIG-MAN-MIB | CISCO-PROCESS-MIB | RFC2982-MIB |
| CISCO-DATA-COLLECTION-MIB | CISCO-PRODUCTS-MIB | RMON-MIB (RFC 1757) |
| CISCO-EMBEDDED-EVENT-MGR-MIB | CISCO-PTP-MIB | RSVP-MIB |
| CISCO-ENHANCED-MEMPOOL-MIB | CISCO-RF-MIB | SNMP-COMMUNITY-MIB (RFC 2576) |
| CISCO-ENTITY-ALARM-MIB | CISCO-RTTMON-MIB | SNMP-FRAMEWORK-MIB (RFC 2571) |
| CISCO-ENTITY-EXT-MIB | CISCO-SONET-MIB | SNMP-MPD-MIB (RFC 2572) |
| CISCO-ENTITY-FRU-CONTROL-MIB | CISCO-SYSLOG-MIB | SNMP-NOTIFICATION-MIB (RFC 2573) |
| CISCO-ENTITY-SENSOR-MIB | DS1-MIB (RFC 2495) | SNMP-PROXY-MIB (RFC 2573) |
| CISCO-ENTITY-VENDORTYPE-OID-MIB | ENTITY-MIB (RFC 4133) | SNMP-TARGET-MIB (RFC 2573) |
| CISCO-FLASH-MIB | ENTITY-SENSOR-MIB (RFC 3433) | SNMP-USM-MIB (RFC 2574) |
| CISCO-FTP-CLIENT-MIB | ENTITY-STATE-MIB | SNMPv2-MIB (RFC 1907) |
| CISCO-IETF-ISIS-MIB | EVENT-MIB (RFC 2981) | SNMPv2-SMI |
| CISCO-IETF-PW-ATM-MIB | ETHERLIKE-MIB (RFC 3635) | SNMP-VIEW-BASED-ACM-MIB (RFC 2575) |
| CISCO-IETF-PW-ENET-MIB | IF-MIB (RFC 2863) | SONET-MIB |
| CISCO-IETF-PW-MIB | IGMP-STD-MIB (RFC 2933) | TCP-MIB (RFC 4022) |
| CISCO-IETF-PW-MPLS-MIB | IP-FORWARD-MIB | TUNNEL-MIB (RFC 4087) |
| CISCO-IETF-PW-TDM-MIB | IP-MIB (RFC 4293) | UDP-MIB (RFC 4113) |
| CISCO-IF-EXTENSION-MIB | IPROUTE-STD-MIB (RFC 2932) | CISCO-FRAME-RELAY-MIB |
| CISCO-IGMP-FILTER-MIB | MPLS-LDP-GENERIC-STD-MIB (RFC 3815) | |

MIB Documentation

To locate and download MIBs for selected platforms, Cisco IOS and Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following location: <http://tools.cisco.com/ITDIT/MIBS/servlet/index>. To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at the following location: <http://tools.cisco.com/RPF/register/register.do>

Open Source License Notices

For a listing of the license notices for open source software used in Cisco IOS XE 3S Releases, see the documents accessible from the License Information page at the following location:

http://www.cisco.com/en/US/products/ps11174/products_licensing_information_listing.html

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 2

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

This chapter describes the new hardware and software features supported in Cisco IOS XE Dublin 17.11.x.

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, on page 15](#)
- [What's New in Software for Cisco IOS XE Dublin 17.11.1a, on page 15](#)

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

There are no new features in this release.

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

| Feature | Description |
|-----------------------------------|---|
| CEM | |
| Support for 3-in-24 BERT patterns | Support for 3-in-24 BERT patterns on the following interface modules and modes: <ul style="list-style-type: none">• 48-port T1 or E1 interface module• 48-port T3/E3 interface module• 1-Port OC-48 or 4-Port OC-12/OC-3 interface module• NCS 4200 Combo 8-Port SFP GE and 1-Port 10 GE 20G Interface Module (NCS4200-1T8S-20CS)• STS-1 mode |

| Feature | Description |
|---|---|
| System CESoP NxDS0 BERT | <p>You can configure BERT patterns at the DS0 level on the following interface modules for both the system and line directions.</p> <ul style="list-style-type: none"> • 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 • NCS 4200 Combo 8-port SFP GE and 1-port 10 GE 20G interface module <p>You can configure speed with bandwidth of 56 kbps or 64 kbps along with the BERT pattern.</p> <p>With DS0 level BERT configuration, you can verify the end-to-end connectivity.</p> |
| Frame Relay Port Mode | <p>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.</p> <p>You can configure HDLC or FR port mode on the following interface modules:</p> <ul style="list-style-type: none"> • NCS4200-3GMS and NCS4200-1T8S-20CS |
| Layer 3 Termination for Frame Relay | <p>You can configure layer 3 termination on the Frame Relay (FR) and Multilink Frame Relay (MFR) sub interface for the following interface modules:</p> <ul style="list-style-type: none"> • NCS4200-3GMS • NCS4200-1T8S-20CS <p>You can assign IP address on the FR sub interface and terminate the Layer 3 traffic where ever required in the network.</p> <ul style="list-style-type: none"> • Layer 3 Termination for Frame Relay • Multilink Frame Relay (MFR) Layer 3 Termination |
| IP Routing: BFD | |
| Micro BFD Support on Port Channel with EFPs | <p>A Micro Bidirectional Forwarding Detection (Micro-BFD) session can detect failures in member links of a port channel. You can now enable Micro-BFD sessions for a port channel on which Ethernet flow Point (EFP) or service instance is configured. This feature ensures that traffic is forwarded to a member link only when the micro-BFD session for that member link is in the UP state.</p> <p>As part of this feature, the source-service-instance number keyword has been added to the port-channel bfd command. The specified service instance provides the source IP address for the micro-BFD session.</p> |

| Feature | Description |
|---|---|
| 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. |
| Programmability | |
| gNMI Dial-Out Using gRPC Tunnel Service | <p>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.</p> <p>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.</p> <p>The following commands are introduced for the tunnel and target configurations respectively:</p> <ul style="list-style-type: none"> • gnxi grpctunnel destination <i>server name</i> • gnxi grpctunnel target |
| 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 | <p>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.</p> <p>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.</p> <p>For more information on how to migrate to stronger cryptographic algorithms for SNMP, see the Field Notice Number: FN72509.</p> <p>For more information on how to migrate to stronger cryptographic algorithms for SSH, see Field Notice Number: FN72511.</p> |
| YANG | |

| Feature | Description |
|--|--|
| YANG Support for show l2vpn atom vc detail Command | <p>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:</p> <p>Cisco-IOS-XE-l2vpn-oper/l2vpn-oper-data/l2vpn-services/l2vpn-atom-vc-info</p> <p>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.</p> <p>In earlier releases, you could perform this action by using the following CLI:</p> <p>show l2vpn atom vc detail</p> <p>Note There is existing YANG support for the following related CLIs in the Cisco-IOS-XE-l2vpn-oper native model:</p> <ul style="list-style-type: none"> • show l2vpn service xconnect peer peer_id vcid vcid • show l2vpn atom commands <p>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.</p> |



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 19](#)
- [Open Caveats - Cisco IOS XE Dublin 17.11.1a, on page 20](#)
- [Cisco Bug Search Tool, on page 21](#)

Resolved Caveats - Cisco IOS XE Dublin 17.11.1a

| Identifier | Headline |
|----------------------------|---|
| CSCwc80493 | APS - K2 byte not reflecting proper value during LRDI and LAIS conditions. |
| CSCwd87661 | Router Fan running at high speed and creating noise(Fan PID A903-FAN-H) - SW version 17.03.04 |
| CSCwd16666 | Ony 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 |
| CSCwd66728 | The uea_mgr crash seen with uea_brcm_update_hw_stats |
| CSCwd38074 | Alarm reporting to IOS and L-bit propagation missing with STS-1E, CT-3, and E1 mode |

| Identifier | Headline |
|----------------------------|---|
| CSCwe19162 | RSP3: After SSO, False Alarm on CNAAP |
| CSCwd11926 | Need support for dual options in CLI for setting clock rate for x21 |
| CSCwd09785 | Overhead DCC tunnel pseudowire not working in port 8 of NCS4200-1T8S-10CS |
| CSCwc41115 | APS 1+1 Uni - Tx K2 to reflect Rx K1 channel number |
| CSCwd28121 | STS-1E & CT-3:E1 loopback syslog and alarm reporting issues |
| CSCwd28107 | RSP3: Bundle rommon version 15.6(57r)S to polaris_dev |
| CSCwc65971 | RSP3: MPLS pseudowire - Incorrect label stack pushed to packet |
| CSCwd05100 | IM booting up on unsupported slot |
| CSCwd04198 | When configurations are pasted in a specific order, line config is missing |
| CSCwd16099 | Not able to unconfigure channel-group under STS-48c when 192 STS are used |
| CSCwd26330 | IMA3G does not generate FEBE's when BPV, P-bit, C-bit error are detected on the T3 port |
| CSCwd48164 | EVPN statd resource leak after protocol flaps |
| CSCwd44817 | After router reload E1 framing gets changed to unframed in SDH VC12 mode with channel-group config |
| CSCwc10211 | IMSG: Random VT's are down with LP_AIS due to Peer IMOIR with scale config with AU-4/tug-3/vc11-T1 |
| CSCwe13024 | RSP2: All readings for Power supply unit reflect as zero though the unit is functional |
| CSCwd67723 | In IMA32D/IMA8D card, sometimes change in E1 controller config(after ctrlr flap) results in IM reboot |
| CSCwd26357 | rs485 with half-duplex configuration when reloaded, it gets into default full-duplex mode |
| CSCwd86980 | High traffic drop is observed on RPFO |
| CSCwb68238 | CSPN SSH requirement |

Open Caveats - Cisco IOS XE Dublin 17.11.1a

| Identifier | Headline |
|----------------------------|---|
| CSCwd88680 | High Convergence after Port channel member failure. |
| CSCwd05362 | Performance issue on router platform. |

| Identifier | Headline |
|----------------------------|---|
| CSCwe42290 | Netconf intermittent connection issue due to checksum issue. |
| CSCwe34672 | High CPU on ptp_uea process. |
| CSCwe33848 | RSP3: Micro-bfd failed when trunk EFP is configured on the port channel |

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>

