Release Notes for Cisco NCS 4206 and Cisco NCS 4216 Series, Cisco IOS XE Amsterdam 17.3.x

First Published: 2020-10-30

Last Modified: 2023-09-29

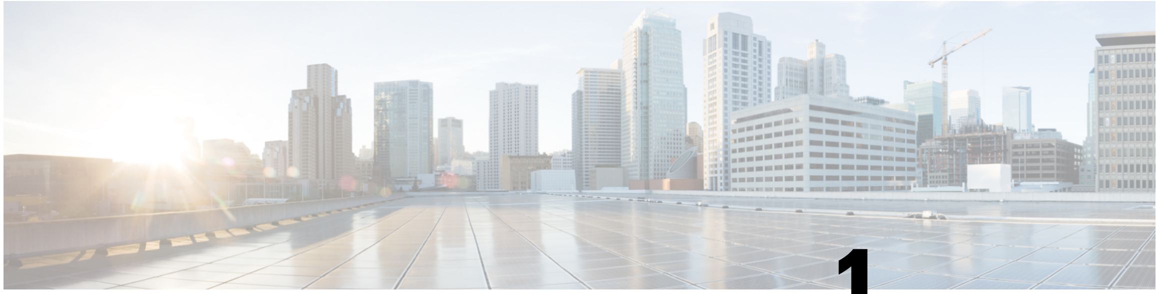
Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1

CHAPTER 2



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

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 it's 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.

NCS 4216 14RU

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 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 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 GigabitEthernet 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.

Swapping of Interface Modules

The following Ethernet interface modules support swapping on the Cisco NCS4216-RSP module:

Use the **hw-module subslot default** command before performing a swap of the modules to default the interfaces on the interface module.

- SFP Combo IM—8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet (1X10GE)
- 2-port 40 Gigabit Ethernet Interface Module (2X40GE)
- 8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module
- 8-port 10 Gigabit Ethernet Interface Module (8X10GE)
- 1-port 100 Gigabit Ethernet Interface Module (1X100GE)
- 2-port 100 Gigabit Ethernet (QSFP) Interface Module (2X100GE)

Use of **hw-module subslot default** command is not supported on the following interface modules.

- 1-port OC-192 Interface Module with 8-port Low Rate CEM Interface Module (10G HO / 10G LO)
- 48 T1/E1 TDM Interface Module (48XT1/E1)
- 48 T3/E3 TDM Interface Module (48XT3/E3)
- 1-port OC48/ 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)
- NCS 4200 Combo 8-Port SFP GE and 1-Port 10 GE 20G Interface Module (NCS 4200-1T8S-20CS)

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.

Table 3: NCS4216-RSP Supported Interface Modules and Part Numbers

RSP Module	Interface Modules	Part Number	Slot
NCS4216-RSP	SFP Combo IM—8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet (1X10GE)	NCS4200-1T8LR-PS	2,5,6,9,10,13,14,15
	1-port 100 Gigabit Ethernet Interface Module (1X100GE)	NCS4200-1H-PK	7, 8
	2-port 100 Gigabit Ethernet (QSFP) Interface Module (2X100GE)[5]	NCS4200-2H-PQ	7, 8
	2-port 40 Gigabit Ethernet QSFP Interface Module (2X40GE)	NCS4200-2Q-P	3,4,7,8,11,12
	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	All slots
	1-port OC48[6]/ 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	All slots
	8-port 10 Gigabit Ethernet Interface Module (8X10GE)	NCS4200-8T-PS	3,4,7,8,11,12

	1-port OC-192 Interface Module with 8-port Low Rate CEM Interface Module (5G/ 10G HO / 10G LO)	NCS4200-1T8S-10CS	3,4,7,8,11,12 (10G mode)
			0,1,2,5,6,9,10,13,14,15 (5G mode)
			Note To enable this IM on slot 0 or slot 1, do the following and reload the router:
			`Router# configure t`
			`Router(config)# license feature service-offload enable`

	NCS 4200 1-Port OC-192 or 8-Port Low Rate CEM 20G Bandwidth Interface Module	NCS4200-1T8S-20CS	3,4,7,8,11,12 (20G mode)
			0,1,2,5,6,9,10,13,14,15 (10G mode)
			Note To enable this IM on slot 0 or slot 1, do the following and reload the router:
			`Router# configure t`
			`Router(config)# license feature service-offload enable`

	48-port T1/E1 Interface module	NCS4200-48T1E1-CE	2,3,4,5,6,7,8,9,10,13,14,15

RSP Module	Interface Modules	Part Number	Slot
	48-port T3/E3 Interface module	NCS4200-48T3E3-CE	2,3,4,5,6,7,8,9,10,13,14,15

[5] IM supports only one port of 100G with RSP3 as QSFP28 on Port 0 in both slots 7 and 8.
[6] If OC48 is enabled, then the remaining 3 ports are disabled.

Cisco NCS 4216 F2B Supported Interface Modules

For information on supported interface modules, see Supported Interface Modules.

Swapping of Interface Modules

The following interface modules support swapping on the Cisco NCS4216-RSP module:

Use the **hw-module subslot default** command before performing a swap of the modules to default the interfaces on the interface module.

- SFP Combo IM—8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet (1X10GE)
- 2-port 40 Gigabit Ethernet Interface Module (2X40GE)
- 8-port 10 Gigabit Ethernet Interface Module (8X10GE)
- 1-port 100 Gigabit Ethernet Interface Module (1X100GE)
- 2-port 100 Gigabit Ethernet Interface Module (2X100GE)
- 8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module

Use of **hw-module subslot default** command is not supported on the following interface modules.

- 1-port OC-192 Interface Module with 8-port Low Rate CEM Interface Module (10G HO / 10G LO)
- 48-port T1/E1 TDM Interface Module (48XT1/E1)
- 48-port T3/E3 TDM Interface Module (48XT3/E3)
- 1-port OC48/ 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)
- NCS 4200 Combo 8-Port SFP GE and 1-Port 10 GE 20G Interface Module (NCS 4200-1T8S-20CS)

Use the **hw-module subslot default** command before performing a swap of the modules to default the interfaces on the interface module.

See the *Cisco NCS 4216 Router Hardware Installation Guide* for information on Supported Interface Modules on the RSP.

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.

Table 4: Cisco NCS4216-RSP Supported Interface Modules and Part Numbers

RSP Module	Interface Modules	Part Number	Slot
NCS4216-RSP	SFP Combo IM—8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet (1X10GE)	NCS4200-1T8LR-PS	2,5,6,9,10,13,14,15
	1-port 100 Gigabit Ethernet Interface Module (1X100GE)	NCS4200-1H-PK	7,8
	2-port 100 Gigabit Ethernet (QSFP) Interface Module (2X100GE)[7]	NCS4200-2H-PQ	7,8
	2-port 40 Gigabit Ethernet QSFP Interface Module (2X40GE)	NCS4200-2Q-P	3,4,7,8,11,12
	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	All slots
	8-port 10 Gigabit Ethernet Interface Module (8X10GE)	NCS4200-8T-PS	3,4,7,8,11,12
	1-port OC-192 Interface Module with 8-port Low Rate CEM Interface Module (5G/ 10G HO / 10G LO)	NCS4200-1T8S-10CS	3,4,7,8,11,12 (10G mode) 0,1,2,5,6,9,10,13,14,15 (5G mode)
	NCS 4200 1-Port OC-192 or 8-Port Low Rate CEM 20G Bandwidth Interface Module	NCS4200-1T8S-20CS	3,4,7,8,11,12 (20G mode) 0,1,2,5,6,9,10,13,14,15 (10G mode)
	48XT1/E1 Interface module	NCS4200-48T1E1-CE	2,3,4,5,6,7,8,9,10,13,14,15
	48XT3/E3 Interface module	NCS4200-48T3E3-CE	2,3,4,5,6,7,8,9,10,13,14,15
	1-port OC48[8]/ 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	All slots

[7] IM supports only one port of 100G with RSP3 as QSFP28 on Port 0 in both slots 7 and 8.
[8] If OC48 is enabled, then the remaining 3 ports are disabled.

Restrictions and Limitations for Cisco NCS 4206 and Cisco NCS 4216

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.

- In the Cisco IOS XE 16.12.1 release, IPSec is not supported on the Cisco RSP3 module.
- VT PMON is not supported.
- APS is supported across interface modules. But it is not supported on the same interface module.
- VT loopback is not supported if T1 is configured for the VT mode.
- DS1/DS3 SF/SD is not supported.
- Alternate 0's and 1's BERT pattern is not supported for DS1.
- All zeros BERT pattern on system side does not get in sync on DS3.
- DS3/OCx MDL does not interoperate with legacy Q.921 standards.
- APM is not supported with EPAR on CEP.
- FDL is not supported.
- STS24-c is not supported on 1-port OC-192 or 8-port low rate CEM interface module.
- Port restriction on 1-port OC-192 or 8-port low rate CEM interface module. If you have OC-48 configured on a port, you cannot use the neighboring port.
- Bellcore remote loopbacks are not supported for DS1/DS3. Only T1.403 remote loopbacks are supported.
- CEP MIB is not supported.
- HSPW is not supported on DS3/DS1/OCX card.
- The **ip cef accounting** command is not supported on the chassis.

- Crash may be observed on the chassis when EoMPLS, CEM, ATM and IMA Pseudowire Redundancy (PW-redundancy) configurations exist while switchover and fail back of the pseudowires are being triggered, and the **show platform hardware pp active pw eompls** command is executed.
- 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 chassis. 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 Cisco NCS 4206. A reload of the chassis 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 of T1, T3, and CT3 circuits to UPSR are not supported.
- DCC is supported only on PPP encapsulation. It is not supported on CLNS encapsulation.
- If oversubscription is enabled on 8-port 10 Gigabit Ethernet interface module, PTP is not supported.
- Effective with Cisco IOS XE Everest 16.6.1, the Port-channel (PoCH) scale is reduced to 24 from 48 for Cisco ASR 900 RSP3 module.

Note The PoCH scale for Cisco NCS 4216 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.
- 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.
- One Ternary Content-Addressable Memory (TCAM) entry is utilized for Segment Routing Performance Measurement. This is required for the hardware timestamping to function.
- 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 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. This is applicable to Cisco NCS 4206 and Cisco NCS 4216 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.

- 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 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 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.

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 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.

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 5: Supported FPGA Versions for NCS 4206-RSP3 and NCS 4216

	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	8x10G FPGA	2x40G FPGA	1x100G FPGA
IM FPGA	3.18SP	1.22	1.22	1.12	—	—	0.17 (0x1100 H)	0.22 (0x1600 H)	0.19 (0x1300 H)
CEM FPGA		4.6	4.6	6.6	—	—	—	—	—
IM FPGA	3.18.1SP	1.22	1.22	1.12	—	—	0.17 (0x1100 H)	0.22 (0x1600 H)	0.19 (0x1300 H)
CEM FPGA		4.6	4.6	7.0	—	—	—	—	—
IM FPGA	16.5.1	1.22	1.22	1.15	—	—	0.21 (0x1500 H)	0.22 (0x1600 H)	0.20 (0x1400 H)
CEM FPGA		0x46310046	0x46310046	5G mode: 0x10070059 10G mode: 0x10050073	—	—	—	—	—
IM FPGA	16.6.1	1.22	1.22	1.15	—	—	0.21 (0x1500 H)	0.22 (0x1600 H)	0.20 (0x1400 H)
CEM FPGA		0x46310046	0x46310046	5G mode: 0x10070059 10G mode: 0x10050073	—	—	—	—	—

	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	8x10G FPGA	2x40G FPGA	1x100G FPGA
IM FPGA	16.7.1	1.22	1.22	1.15	—	2.0	0.21 (0x1500 H)	0.22 (0x1600 H)	0.20 (0x1400 H)
CEM FPGA		0x46410046	0x46410046	5G mode: 0x10780059 10G mode: 0x10120076	—	0x10230039	—	—	—
IM FPGA	16.8.1	1.22	1.22	1.15	—	2.0	0.22	0.22	0.20
CEM FPGA		0x46470046	0x46470046	5G mode: 0x10780059 10G mode: 0x10670075	—	0x10380039	—	—	—
IM FPGA	16.9.1	1.22	1.22	1.15	—	2.0	0.22	0.22	0.20
CEM FPGA		0x50090050	0x50060050	5G mode: 0x10070062 10G mode: 0x10480078	—	0x10520063	—	—	—
IM FPGA	16.10.1	1.22	1.22	1.15	—	2.0	0.22	0.22	0.20
CEM FPGA		0x50090050	0x50060050	5G mode: 0x10070062 10G mode: 0x10480078	—	0x10520063	—	—	—
IM FPGA	16.11.1	1.22	1.22	1.15	—	2.0	0.22	0.22	0.20
CEM FPGA		0x00000051	0x00000051	5G mode: 0x10180062 10G mode: 0x10510078	—	0x10820063	—	—	—

	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	8x10G FPGA	2x40G FPGA	1x100G FPGA
IM FPGA	16.12.1	1.22	1.22	1.15	0.80	2.0	0.22	0.22	0.20
CEM FPGA		0x00000051	0x00000051	5G mode: 0x10180062 10G mode: 0x10510078	10G mode: 0x10260046 20G mode: 0x10710047	0x10050071	—	—	—
IM FPGA	16.12.2	1.22	1.22	1.15	0.80	2.0	0.22	0.22	0.20
CEM FPGA		0x00000051	0x00000051	5G mode: 0x10180062 10G mode: 0x10510078	10G mode: 0x10260046 20G mode: 0x10710047	0x10050071	—	—	—
IM FPGA	17.1.1	1.22	1.22	1.15	0.80	2.0	0.22	0.22	0.20
CEM FPGA		0x52050052	0x52310052	5G mode: 0x10180062 10G mode: 0x10510078	10G mode: 0x10770047 20G mode: 0x10710047	0x10060071	—	—	—
IM FPGA	17.3.1	1.22	1.22	1.15	0.80	2.0	0.22	0.22	0.20
CEM FPGA		0x52050052	0x52310052	5G mode: 0x10180062 10G mode: 0x10510078	10G mode: 0x10770047 20G mode: 0x10710047	0x10060071	—	—	—
IM FPGA	17.3.2a	1.22	1.22	1.15	0.93	2.0	0.23	0.22	0.20
CEM FPGA		0x52050052	0x52310052	5G mode: 0x10180062 10G mode: 0x10510078	10G mode: 0x10770047 20G mode: 0x10710047	0x10060071	—	—	—

	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	8x10G FPGA	2x40G FPGA	1x100G FPGA
IM FPGA	17.3.3	1.22	1.22	1.15	0.93	2.0	0.23	0.22	0.20
CEM FPGA		0x52050052	0x52310052	5G mode: 0x10180062 10G mode: 0x10510078	10G mode: 0x10770047 20G mode: 0x10710047	0x10060071	—	—	—
IM FPGA	17.3.4	1.22	1.22	1.15	0.93	2.0	0.23	0.22	0.20
CEM FPGA		0x52050052	0x52310052	5G mode: 0x10180062 10G mode: 0x10510078	10G mode: 0x10770047 20G mode: 0x10710047	0x10060071	—	—	—
IM FPGA	17.3.5	1.22	1.22	1.15	0.93	2.0	0.23	0.22	0.20
CEM FPGA		0x52050052	0x52310052	5G mode: 0x10180062 10G mode: 0x10510078	10G mode: 0x10770047 20G mode: 0x10710047	0x10060071	—	—	—
IM FPGA	17.3.6	1.22	1.22	1.15	0.93	2.0	0.23	0.22	0.20
CEM FPGA		0x52050052	0x52310052	5G mode: 0x10180062 10G mode: 0x10510078	10G mode: 0x10770047 20G mode: 0x10710047	0x10060071	—	—	—
IM FPGA	17.3.7	1.22	1.22	1.15	0.93	2.0	0.23	0.22	0.20
CEM FPGA		0x52050052	0x52310052	5G mode: 0x10180062 10G mode: 0x10510078	10G mode: 0x10770047 20G mode: 0x10710047	0x10060071	—	—	—

	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	8x10G FPGA	2x40G FPGA	1x100G FPGA
IM FPGA	17.3.8	1.22	1.22	1.15	0.93	2.0	0.23	0.22	0.20
CEM FPGA		0x52050052	0x52310052	5G mode: 0x10180062 10G mode: 0x10510078	10G mode: 0x10770047 20G mode: 0x10710047	0x10060071	—	—	—
IM FPGA	17.3.8a	1.22	1.22	1.15	0.93	2.0	0.23	0.22	0.20
CEM FPGA		0x52050052	0x52310052	5G mode: 0x10180062 10G mode: 0x10510078	10G mode: 0x10770047 20G mode: 0x10710047	0x10060071	—	—	—

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

    For more information, see the Alarm Configuring and Monitoring Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series).

  - 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

- Configuring IEEE 802.3ad Link Bundling is now available in Ethernet Channel Configuration Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series).

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	IPMROUTE-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

New Features

This chapter describes the new hardware and software features supported on the Cisco NCS 4200 Series in this release.

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.

New Hardware Features in Cisco IOS XE Amsterdam 17.3.8

There are no new features in this release.

New Software Features in Cisco IOS XE Amsterdam 17.3.8

There are no new features in this release.

New Hardware Features in Cisco IOS XE Amsterdam 17.3.7

There are no new features in this release.

New Software Features in Cisco IOS XE Amsterdam 17.3.7

There are no new features in this release.

New Hardware Features in Cisco IOS XE Amsterdam 17.3.6

There are no new features in this release.

New Software Features in Cisco IOS XE Amsterdam 17.3.6

There are no new features in this release.

New Hardware Features in Cisco IOS XE Amsterdam 17.3.5

There are no new features in this release.

New Software Features in Cisco IOS XE Amsterdam 17.3.5

There are no new features in this release.

New Hardware Features in Cisco IOS XE Amsterdam 17.3.4

There are no new features in this release.

New Software Features in Cisco IOS XE Amsterdam 17.3.4

There are no new features in this release.

New Hardware Features in Cisco IOS XE Amsterdam 17.3.3

There are no new features in this release.

New Software Features in Cisco IOS XE Amsterdam 17.3.3

There are no new features in this release.

New Hardware Features in Cisco IOS XE Amsterdam 17.3.2a

There are no new features in this release.

New Software Features in Cisco IOS XE Amsterdam 17.3.2a

There are no new features in this release.

New Hardware Features in Cisco IOS XE Amsterdam 17.3.1

Supported Optics

The following optics are supported for the Cisco IOS XE Amsterdam 17.3.1 release:

- ONS-SI-GE-SX=
- ONS-SC+-10G-LR=
- ONS-SC+-10G-SR=
- ONS-SI-GE-ZX=
- ONS-SE-ZE-EL=
- ONS-SC+-10G-ER=
- ONS-SC+-10G-ZR=
- GLC-GE-DR-LX=
- ONS-SE-Z1=

For more information, see the NCS 4206-16 Optics Matrix.

New Software Features in Cisco IOS XE Amsterdam 17.3.1

Feature	Description
Segment Routing	
EVPN Single-Homing Over Segment Routing	The EVPN Single-Homing feature utilizes the BGP MPLS-based Ethernet VPN functionality as defined in RFC 7432. For EVPN Single-Homing, a CE device is attached to a single PE device and has an Ethernet Segment. In Cisco IOS XE Amsterdam 17.3.1 release, EVPN single-homing feature is supported over segment routing.
SR-TE Per-Flow (Class) ODN and Automated Steering (PCE Delegated)	This feature lets you steer traffic with SR-TE PFP based on the QoS markings on the packets. The traffic is then switched onto the appropriate path based on the forward classes of the packet. This feature is supported on the Cisco RSP2 and RSP3 modules.
Segment Routing Flexible Algorithm	Segment Routing Flexible Algorithm allows operators to customize IGP shortest path computation according to their own needs. Custom SR prefix-SIDs are assigned to forward the packets beyond link-cost-based SPF. As a result, a traffic engineered path is automatically computed by the IGP to any destination reachable by the IGP.
Segment Routing Performance Measurement Delay Measurement Using RFC 5357 (TWAMP Light)	This feature enables hardware timestamping. The Performance Measurement (PM) for link delay uses the light version of Two-Way Active Measurement Protocol (TWAMP) over IP and UDP defined in Appendix I of RFC 5357. TWAMP provides an alternative for interoperability when RFC 6374 is not used.
Segment Routing Performance Measurement End-to-End Delay Measurement	This feature allows to monitor the end-to-end delay experienced by the traffic sent over a Segment Routing policy. This feature ensures the delay does not exceed the specified threshold value and violate the SLAs. Use this feature to apply extended TE link delay metric (minimum delay value) to compute paths for Segment Routing policies as an optimization metric or as an accumulated delay bound.
Static Route Traffic Steering Using SR-TE Policy	This feature allows the non colored (BGP Extended Community) prefix to steer traffic over static policy. Prior to this release, only colored (BGP Extended Community) prefix could automatically steer traffic based on the defined policy using a tunnel interface. Unlike non colored prefix, this was possible only for the colored prefix as it could match the SR policy. IPv4 static routes are now enhanced to leverage the SR policies to aid Segment Routing Traffic Engineering (SR-TE). This facilitates traffic steering for non colored prefix as you can now configure IP Static Route with SR static policy. The following new keyword for the **ip route** command is introduced: segment-routing policy [*policy name*]

Feature	Description
Telemetry (Model-Based Telemetry and Event-Based Telemetry) Support for Performance Measurement	This feature enables Model-Based Telemetry (MDT) and Event-Based Telemetry (EDT) that allow the data to be directed to a configured receiver. This data can be used for analysis and troubleshooting purposes to maintain the health of the network. This feature is supported on Cisco ASR 900 RSP3 module. The **sr_5_label_push_enable** SDM template is mandatory for this feature to function.
Alarm Configuring and Monitoring Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series)	
Support for new alarm profile based on the Telcordia profile for chassis	The alarm profile based on Telcordia includes "Service Affecting" information for chassis entities. This information enables you to check the service affecting state for each alarm under a chassis.
Layer 2	
RSPAN over VPLS Pseudowire Network	This feature allows the traffic mirroring destination port to be configured as a pseudowire rather than a physical port. This feature lets the designated traffic on the source port to be mirrored over the pseudowire to a remote location. This feature is supported on the Cisco RSP3 module.
MPLS Traffic Engineering Path Link and Node Protection	
MPLS Point-to-Multipoint Traffic Engineering Support for Static Pseudowires	The Static Pseudowires over Point-to-Multipoint Traffic Engineering (P2MP TE) feature emulates the essential attributes of a unidirectional P2MP service. It can be used to transport layer 2 multicast services from a single source to one or more destinations.
Timing and Synchronization	
Telemetry for GNSS Module	This feature provides externalization of operational data using Network Configuration Protocol (NETCONF) or Yet Another Next Generation (YANG) data modeling language. Prior to this release, the traditional show commands were available to only view the GNSS statistic data. But, you could not use these show command outputs to manage network devices as demanded by centralized orchestration application such as Cisco Digital Network Architecture Center (DNAC). The introduction of this feature helps to bring more visibility in the timing services operations. This feature is supported on Cisco ASR 900 RSP3 module.
1-Port OC-192 or 8-Port Low Rate CEM Interface Module	

Feature	Description
Interworking Multiservice Gateway Access Circuit Redundancy (iMSG ACR) support for NCS 4200 Combo 8-Port SFP GE and 1-Port 10 GE 20G Interface Module (NCS4200-1T8S-20CS)	The iMSG ACR feature is supported on serial interfaces for SONET and SDH ACR. DCC and MS features are also supported.
Pseudowire Scale Support	A maximum of 26,880 CEM Pseudowires are supported on the 1-Port OC-192 or 8-Port Low Rate CEM interface module. This feature is supported on the Cisco RSP3 module.
ACR and DCR Scale Support	Adaptive Clock Recovery (ACR) and Differential Clock Recovery (DCR) are techniques used for Circuit Emulation (CEM) to recover clocks on the Cisco RSP3 module.
DCC Support	The Data Communication Channel (DCC) feature uses the SONET or SDH Operation Administration and Maintenance (OAM) channel to manage devices that support SONET or SDH interfaces on the Cisco RSP3 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	
IP Interworking with VLAN Handoff	VLAN handoff enables the support for IP interworking Pseudowire. IP interworking Pseudowire enables the service provider to terminate the TDM circuit early in the network and transport the IP payload on HDLC, PPP, or MLPPP links, over the MPLS core to the Ethernet network.
Interworking Support for nxDS0	Interworking function (IWF) for PPP/HDLC is supported on Ethernet for E1/STM1 ports. This support is extended at nxDS0 level to speed up the GSR TDM migration.
MLPPP ACR support for IPv4 or IPv6 Interworking Multiservice Gateway (iMSG)	MLPPP ACR is supported for IPv4 or IPv6 iMSG on the Cisco RSP3 module. The restrictions for MLPPP interworking are applicable to iMSG ACR.
IP Multicast: Multicast	
Aggregated Interface Statistics on Bundle	Aggregate multicast packet count is implemented for all the (S,G) entries for which the given BDI serves as the OIF.
Native Multicast SLA Measurement with MLDP	Outgoing interface (OIF) statistics in a native multicast setup implements an extra output to include the packet count sent over the (S,G) entry and the traffic rate.
Quality of Service	

Feature	Description
CoS Conditional Marking	This feature lets you implement the CoS marking on the basis of the Traffic class and the Drop precedence. This feature is supported on the Cisco RSP3 module.

Other Supported Features in this Release

- SyncE YANG module Telemetry integration
- On-change notifications for TLDP
- On-change notifications for Interface (including tunnels) state
- KGV E2E Solution
- SRTE-PM-OPER-on-change notification
- On-Change Notifications for LAG and LACP—The TLDP On-Change Notifications feature notifies the users when TLDP sessions come up or go down and when TLDP is configured or disabled. TLDP must be enabled for the notifications to work. For more information, see the Programmability Guide for Cisco IOS XE Amsterdam 17.3.1.
- Configurable Y.1564 Service Activation Frame Sizes and EMIX Support—Enterprise traffic (EMIX) packet size (default abceg pattern) is supported. For EMIX traffic, ITU-T Rec. Y.1564 packet sizes of 64, 128, 256, 1024, and 1518 bytes are supported. For more information, see the IP SLAs Configuration Guide, Cisco IOS XE 17 (Cisco ASR 4200 Series).
- NCS4200-1H-PK and NCS4200-2Q-P interface modules based FAN OIR—FAN Online Insertion and Removal (OIR) is applicable every time the IM based fan speed profile is switched to the 1-port 100 Gigabit Ethernet Interface Module (1X100GE) and 2-port 40 Gigabit Ethernet QSFP Interface Module (2x40GE) interface modules. For more information, see the Cisco NCS 4206 Hardware Installation Guide.
- Install Workflow based ISSU support—Starting with Cisco IOS XE Amsterdam 17.3.1, Install Workflow based ISSU method is supported on the Cisco RSP3 module. For more information, see the High Availability Configuration Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series).
- Lawful Intercept Enhancement—Prior to Cisco IOS XE Amsterdam 17.3.1 release, only single TAP per interface was supported. Starting with Cisco IOS XE Amsterdam 17.3.1 release, multiple TAPs per interface are supported. For more information on multiple taps, see the System Security Configuration Guide, Cisco IOS XE 17 (Cisco ASR 900 Series).
- HA RF Notification—In networking devices running Single-Switch-On (SSO), both Route Processors (RP) must be running the same configuration so that the standby RP is always ready to assume control if the active RP fails. To achieve the benefits of SSO, synchronize the configuration information from the active RP to the standby RP at start-up and whenever changes to the active RP configuration occur. For more information see the *High Availability Configuration Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series)*.
- ROMMON Upgrade on Cisco RSP3 Module—Routers running a ROMMON version that is lower than version 15.6(33r)S is auto upgraded to version 15.6(33r)S during a router restart. However, if a Cisco IOS XE release with ROMMON image is bundled with a version lower than the running ROMMON version, then the ROMMON is not auto downgraded. For more information, see the *High Availability Configuration Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series)*.

- ROMMON Auto Upgrade—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 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. This is applicable to Cisco NCS 4206 and Cisco NCS 4216 routers. For more information, see the *High Availability Configuration Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series)*.

- Prior to release Cisco IOS XE Amsterdam 17.3.1 on Cisco RSP3 module, for sparse mode (SM) in VRF, rendezvous point (RP) must be in ENCAP PE. This restriction is no more applicable on Cisco RSP3 module. For more information, see the IP Multicast: Multicast Configuration Guide, Cisco IOS XE 17 (Cisco ASR 900 Series).

- Prior to release Cisco IOS XE Amsterdam 17.3.1, in case of Protocol Independent Multicast (PIM) Source Specific Multicast (SSM) with Bridge Domain Interface (BDI) as Incoming Interface (IIF), IGMP snooping was not supported on the corresponding Bridge Domain (BD). And, in case of PIM Sparse Mode (PIM-SM) with Bridge Domain Interface (BDI) as Incoming Interface (IIF), IGMP snooping was not supported on the corresponding BD in non-Designated Router (DR) node. To overcome these restrictions, enable the command **platform multicast bridge-tcam-handling disable** and reload the router. For more information, see the *IP Multicast: Multicast Configuration Guide, Cisco IOS XE 17 (Cisco ASR 900 Series)*.

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.

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

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.8a

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

Open Caveats – Cisco IOS XE Amsterdam 17.3.8a

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.8

There are no resolved caveats for this release.

Open Caveats – Cisco IOS XE Amsterdam 17.3.8

There are no open caveats for this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.7

Identifier	Headline
CSCwa29664	BGP neighbor cannot up with bfd strict-mode configured
CSCwd15539	RSP2/RSP3 : IM's shouldn't reload during sipspa install stage 3 in single step install ISSU

Identifier	Headline
CSCwa33365	SNMP polling for traffic stats is displaying wrong values for all interface

Open Caveats – Cisco IOS XE Amsterdam 17.3.7

Identifier	Headline
CSCwb77396	G.8032: Ring brief output doesn't display the Block port flag in the Idle state.
CSCwb75983	BFD Session with authentication with 16 or more characters remains down
CSCvv06958	CPE SIT: IP Sec tunnel is not reachable after RSP3 SSO
CSCvw47384	Defaulting the g8032 ring ports and reapplying the same config, results the Ring in pending state.
CSCwa30653	MVPN Profile 14 : Data MDT traffic not flowing with 2 paths when OSPF cost configured on 1 path
CSCwb60002	Router may experience an unexpected reset when configuring or using interface BDI &gt;= 4097
CSCvz64063	APS:ACR:Shut before reload and no shut after reload make Active and standby states inconsistent
CSCvv45107	RSP3:%FPD_MGMT-3-PKG_VER_MISMATCH_NOTE is seen during auto-upgrade of celeborn IM
CSCvt99060	RSP3: Warning message display when SR PFP scale tunnels are configured beyond 250
CSCvu16223	VPLS BD configured with MAC limit starts learning MAC address upon VPLS session flap
CSCvx92919	High convergence seen during re-opt scenario with Flex-LSP Non-revertive Config

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.6

Identifier	Headline
CSCwa94444	F2B chassis: The **show environment** command does not display the fan speed.
CSCwa99837	RSP3: Implement show command to display VOQ that failed during delete VOQ.
CSCwa54842	RSP3: QOSMGR-4-QUEUE_ExCEEDING_HW: VOQs exceeded hardware limit.
CSCwb06353	Router goes down with IP SLA configuration which is not supported.
CSCvy34396	MAC table inconsistency due to parity error.

Identifier	Headline
CSCwb77723	Duplicated unicast ARP packets.
CSCvx26935	VOQ deletion failure due to the queue 'nonempty' state.
CSCwb01940	The router drops L2 multicast traffic upon REP topology change.
CSCwb01224	Multihop BFD transit packets getting dropped the router after upgrade to 17.3.3.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.6 - Platform Independent

Identifier	Headline
CSCwb66047	RSP3/ASR920/RSP2:node crashed @ l2rib_obj_peer_tbl_cmd_print

Open Caveats – Cisco IOS XE Amsterdam 17.3.6

Identifier	Headline
CSCvw47384	Setting the g8032 ring ports to the default value and reapplying the same configuration, results the Ring to a pending state.
CSCwb60002	The router experiences an unexpected reset when configuring or using an interface with BDI value greater than or equal to 4097.
CSCwb60655	RSP2: Interface remains down after SSO or ISSU upgrade.
CSCvz02262	TCAM corruption happening at bank boundary when one of the bank is full.
CSCvz64063	APS:ACR:Shut before reload and no shut after reload make Active and standby states inconsistent

Open Caveats – Cisco IOS XE Amsterdam 17.3.6 - Platform Independent

Identifier	Headline
CSCvu15652	CEM26K : confiig / unconfig of CEME26K circuits causes 1-2 ckts in down state in standby RSP3.
CSCvv74332	ASR920:VPLSoBKPW:MAC not flushed/withdrawn in remote peer on VC swichover from active to standby.

Identifier	Headline
CSCwa30653	MVPN Profile 14 : Data MDT traffic not flowing with 2 paths when OSPF cost configured on 1 path
CSCvu06350	16.12.3 ES: Active RP crashed due to UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BFD events
CSCvw19225	[17.5 EIGRP] Deleting bgp config does not remove the redistribute vrf CLI under Eigrp process
CSCwc25454	SSH to IPv6 LinkLocal address don't work without explict "ip ssh source-interface" configuration

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.5

Identifier	Headline
CSCvz20710	ASR903/ASR907 A900-IMA1Z8S-CXMS EIGRP flapping on framing SDH Serial interface.
CSCvz07477	DWDM SFPs threshold Value set to 0.0 dbm for RX/TX and -0.0 C for temperature.
CSCvy43352	A900-IMA1Z8S-CXMS IM is not reloading during ISSU even though CEM FPGA version have a mismatch.
CSCvy35769	ACR DCR recovered-clock is FREERUN after SSO in eomer T3 port.
CSCvy26121	Object down failures observed on ASR903 devices post upgrade to 16.12.3.
CSCvy25392	Cannot delete recovered clock configuration from STS-3c.
CSCvy82376	IMs on slots 13, 14 and 15 out of service on ASR-907 chassis.
CSCvy50955	CEM traffic not resuming after IM shut/unshut with Service inst on Gig created when TDM IM is shut.
CSCvy66426	RSP3: Code hardening: Delays between SPI Flash operation during IO FPGA upgrade.
CSCvy92074	MTU programming for mpls l2 vc may fail after interface flaps.
CSCvz20857	STS1E controller bay/port is wrong in controller UPDOWN syslog during T3 alarm.
CSCvz20865	A900-IMA1Z8S-CXMS in HA setup and with APS, configure 5376 VT15 T1 cem circuit, Error observed for last path.
CSCvz57242	ASR90x-RSP3 : IP MTU wrongly programmed in ASIC after removing/reconfiguring the ip address.
CSCvz37014	ICMP Jitter: Incorrect timestamping : registry to use/update receive timestamp for rsp3 platform.
CSCvz19022	ASR 903 RSP3C 16.9.3 and 16.12.3 Ping issue with MTU greater than 1508.
CSCwa06605	With port channel flaps kbp counts increasing and leading to leak.

Identifier	Headline
CSCvy64788	LLC frames are getting looped back due to autonomic networking.
CSCwa09302	The iMSG serial interfaces bitrate/sec data is displayed incorrectly in show command output.
CSCwa04795	Interfaces are showing up in SNMP polling while associated hardware does not exist on system.
CSCvx32380	RSP3 : SFP GLC-FE-100LX-RGD show incorrect description.
CSCvy51848	Active RP HW started booting in loop during an IO FPGA upgrade and standby.
CSCvy29290	ASR90x-RSP3 : Pending objects for BDI Tx Channel on creation of Port channel with member link.
CSCvz79672	HQoS on egress TenGig interface is not working properly.
CSCvz49468	APS:ACR traffic fails after ISSU from 16.12 to 17.3.
CSCvy23345	ASR90X-RSP3: MAC address is getting learned for L2CP control frames over the G.8032 blocked port.
CSCvz09447	The IMA1Z8S-CX-MS protection switching on LOS condition disrupts service for greater than 200 msec.
CSCvy78284	The router will crash when zeroised RSA key is regenerated.
CSCvz62438	ASR90x-RSP3: BDI routing frames corrupted on deletion and recreation of EFP.
CSCwa41638	The router MAC table and L2VPN EVPN table are out of sync.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.5 - Platform Independent

Identifier	Headline
CSCvy91369	IOS-XE : IPSLA ICMP-Jitter over L3VPN results incorrect jitter value.
CSCvz25471	ASR903/920: NSO config push failure seen due to getconf on BD gives additional value “mac learning”
CSCvy56660	mlacp backbone interface defined in netconf as Container instead of list entry

Open Caveats – Cisco IOS XE Amsterdam 17.3.5

Identifier	Headline
CSCvy34396	MAC table inconsistency due to parity error.

Identifier	Headline
CSCwa64889	Wrong L3-Programming for BDI
CSCvz02262	TCAM corruption happening at bank boundary when one of the bank is full.
CSCvz64063	APS:ACR:Shut before reload and no shut after reload make Active and standby states inconsistent

Open Caveats – Cisco IOS XE Amsterdam 17.3.5 - Platform Independent

Identifier	Headline
CSCwa36608	RSP3 ICCP stuck on CONNECTING state after RSP SO on Active PoA

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.4

Caveat ID Number	Description
CSCvv99456	ACL entries with FRAGMENT keywords are not working
CSCvy82320	DHCP packets are getting dropped in case snooping is enabled

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.4 - Platform Independent

Caveat ID Number	Description
CSCvy04023	Netconf datastore PTP data may unsync from running configuration

Open Caveats – Cisco IOS XE Amsterdam 17.3.4

Caveat ID Number	Description
CSCvy04090	Intermittent blackholing of traffic due to CEF table corruption
CSCvy21560	All IM cards in INSERTED state on performing ISSU 16.9.3 to 16.12.3
CSCvy25392	Cannot delete recovered clock configuration from STS-3c
CSCvy26121	Object down failures observed on routers post upgrade to 16.12.3

Caveat ID Number	Description
CSCvy29290	Pending objects for BDI Tx Channel on creation of Port channel with member link

Open Caveats – Cisco IOS XE Amsterdam 17.3.4 - Platform Independent

There are no new Platform Independent Open Caveats for this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
CSCvv83093	OBFL updation with valid time after NTP Sync in RTC failure case
CSCvv95745	Crash of standby supervisor because of QoS Overhead Accounting
CSCvw04366	UEA: Display GNSS Chassis SN instead of PCB SN in show CLI
CSCvw34109	PTP failure due to LSMPI buffer exhaustion
CSCvw48885	IM OIR as part of ISSU resulted in IOSD Crash for T3E3 RSP3 IM
CSCvw58359	8275.1/2 Node is crashing when more than 8 Dynamic ports are created

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.3 - Platform Independent

Caveat ID Number	Description
CSCvg75709	Unnecessary RIB updates when metric-style transition is configured.
CSCvv40006	Traceback: IP SLA triggers INJECT_HDR_LENGTH_ER and INJECT_FEATURE_ESCAPE log message
CSCvv79677	ASR902-RSP2 crashed after BGP flaps
CSCvv91741	Resequencing ACL with remarks only resequences permit or deny entries, remarks not changed.
CSCvw05035	BGP fall-over not working when Null0 static route is configured
CSCvw19062	Changing external route tag does not update origin code in BGP
CSCvw37109	Pseudowire interface may be unexpectedly removed from VFI on unrelated configuration change

Caveat ID Number	Description
CSCvw86336	Unsupported interfaces for logging event link-status needs to be removed in mapping

Open Caveats – Cisco IOS XE Amsterdam 17.3.3

There are no open caveats for this release.

Open Caveats – Cisco IOS XE Amsterdam 17.3.3 - Platform Independent

Caveat ID Number	Description
CSCvu15652	CEM26K: confiig / unconfig of CEME26K circuits causes 1-2 ckts in down state in standby RSP3.
CSCvu77385	[SVSP-457]-Full throughput not working priority shaper percent is > ~40 over 100g nni
CSCvv71209	RSP3: MTU changes on access interface causing low memory and stby RSP crash
CSCvv86988	NCS4200-3GMS: standby rp iosd crashes continuously when serial acr nxds0 configs are applied
CSCvw54661	ASR920: HS2 node is chasing with core generation and core pointing to EFP process.
CSCvw77485	Router may not send PIM Register message if RP is reachabile over TE tunnel

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.2a

Caveat ID Number	Description
CSCvt58155	RSP3c: Kernel crash bcmINTR rcu_check_callback
CSCvt82525	ASR 900 crash while IPV6 updating prefixes
CSCvu16135	STS1E : Remote loopback not working under sts1e controller
CSCvu18276	ASR903 Standby RSP3 crash during IOS upgrade
CSCvu36636	ASR900 ROMMON region 0 and 1 verification CLI
CSCvu66126	OC192 APS Group Stuck with Signal Fail condition
CSCvu83291	Memory leak due to QoS policer
CSCvu95940	RSP2:Egress QoS policy config missing on PoCh member link flap

Caveat ID Number	Description
CSCvv13495	17.1.1. Loopback local not working on T3 card protection physically connected ports
CSCvv14816	MVPN_GRE mcast traffic loss on local receivers and across VRF after Access BDI flap
CSCvv16454	Traffic failure due to MPLS ECMP load-balancing in one of the labelled path
CSCvv23067	ISSU is failing with lookup failure in APS48 five group setup from 16_9_4 to 17_3_1 images
CSCvv24059	Crash is noticed on RSP when EMPLSINTD is exhausted.
CSCvv34831	L2 mcast vpls forwarding outage caused by rep ring changes
CSCvv42595	REP flapping randomly and frequently due to port down
CSCvv85503	MVPN GRE traffic drop for few prefixes
CSCvv51145	Crash seen on \"show plat hard pp active feature multicast database ipv4 table label 756 eos 0\"

Resolved Caveats – Cisco IOS XE Gibraltar 17.3.2a - Platform Independent

Caveat ID Number	Description
CSCvc33357	Incorrect BC value under show policy-map when User defined percentage based CIR is defined

Open Caveats – Cisco IOS XE Amsterdam 17.3.2a

Caveat ID Number	Description
CSCvv95745	Crash of standby supervisor because of QoS Overhead Accounting
CSCvw34109	PTP failure due to LSMPI buffer exhaustion

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.1

Caveat ID Number	Description
CSCvn47496	ENH : RSP3C Request for overriding restriction "MVPN-GRE VRF-SM: RP must be at Encap PE"

Caveat ID Number	Description
CSCvq64605	RSP3: RLFA resource leak on FRR create/delete with link flaps
CSCvs21698	I2C stuck/bad IM/OIR causing rsp3c(both) to reload at "cmanrp_chasfs_spa_oir_remove"
CSCvs25451	Telemetry config Vanish after SSO
CSCvs62447	Netconf login via loopback int is failing though it is working with other inband int
CSCvs63874	Reworked: Invalid ifindex during notification causing lldp localport table mib walk failure
CSCvs71834	Stops forwarding over VC after dot1.q tag is removed and added back to service instance
CSCvs85331	QSFP-100G-LR4-S optical sensors not shown in CISCO-ENTITY-SENSOR-MIB
CSCvs89777	Change alarm threshold values for 8x10G IM
CSCvt35963	Uea_mgr and keepalive crashes observed in a sequence after attempting to enable service-offload
CSCvt53795	CPG: OIR of Primary and Backup IM same time does not update LINK_PTR in MCDB and causes Traffic Drop
CSCvt58665	Baseline : after shut and no shut LOS is not cleared from controller
CSCvt64706	CPU HOG due to constant soft-parity errors
CSCvt98075	Memory leak seen on SNMP DG when IGP flaps
CSCvu30972	All readings for power supply unit reflect as zero though the unit is functional
CSCvu31393	[RSP3-poch-Mcast]: igmp queries are not egressing out of poch in a sequence
CSCvu51472	Support for SAToP payload 64 byte and dejitter 2 ms in LOTR IMs
CSCvt56447	Since UPSR is unsupported for STS1e, need to block CLI structure for user to configure
CSCvt88660	CT3 channelized T1s are not displayed under show command of STS1e virtual controller with card protection
CSCvt90530	Let the Oper status for STS1E virtual controller to be displayed in upper case as "UP" for show cmd
CSCvu62934	For card protection 1+1, naming convention not proper for LOP STS-1 1, VTG 1, VT 3
CSCvv17231	When mode VT1-15 is configured on card protected STS1E controller, can see discrepancy in LOP O/P
CSCvu61765	BERT statistics not seen in &ldquo;show controller STS1E&quot; with mode unframed

Open Caveats – Cisco IOS XE Amsterdam 17.3.1

Caveat ID Number	Description
CSCvt58155	rsp3c: Kernel crash bcmINTR rcu_check_callback
CSCvt82525	Crash while IPV6 updating prefixes
CSCvu03137	Removing and reconfiguring rtp-present in bulk causing CEM ckt in standby goes DN
CSCvu18276	Standby RSP3 crash during IOS upgrade
CSCvu36636	ROMMON region 0 and 1 verification CLI
CSCvu55571	CEM Scale:Removing and reconfiguring rtp-present in bulk causing ssm provisioning failure in standby
CSCvu74741	MVPN GRE : Mcast traffic forwarding fails randomly for few prefixes due to PIM registration issues
CSCvv49690	With mode VT1-15 on STS1E controller, LOP is in UP state even though Controller and HOP is down
CSCvw34109	PTP failure due to LSMPI buffer exhaustion