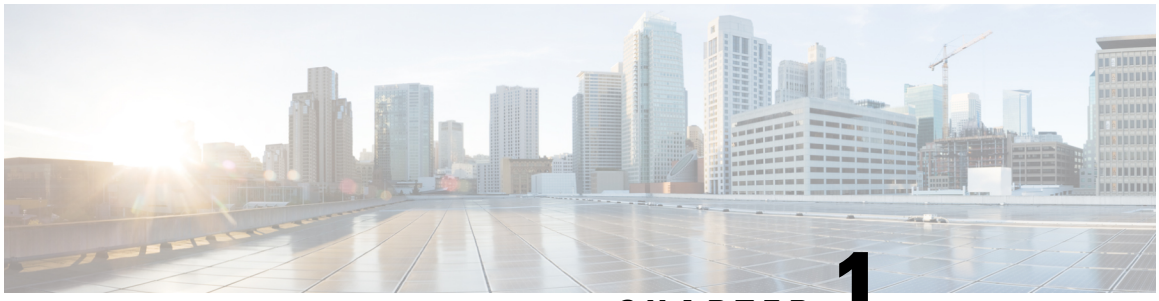
Release Notes for Cisco NCS 4206 and Cisco NCS 4216 Series, Cisco IOS XE Bengaluru 17.6.x

First Published: 2021-11-30

Last Modified: 2024-03-15

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

CONTENTS



CHAPTER 1

Introduction

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

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

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.

- From the Cisco IOS XE 16.5.1 and 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 port within this port group is configured with OC48 rate, the other port cannot be used.
- RS422 pinout works only on ports from 0 to 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.
- 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.
- 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.

- 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 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 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 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.
- Test Access Port (TAP) is not supported when the iMSG VLAN handoff feature is enabled on the same node.
- SF and SD alarms are not supported on T1 and T3 ports for the following interface modules:

- NCS4200-3GMS
- NCS4200-48T3E3-CE
- NCS4200-48T1E1-CE

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 TDM IM and CEM FPGAs 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
IM FPGA	17.6.7	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	17.6.6a	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	17.6.6	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	17.6.5	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	17.6.4	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

	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	17.6.3	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	17.6.2	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 6: 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
17.6.7	—	69.32	—	—	—	—	—
17.6.6a	—	69.32	—	—	—	—	—
17.6.6	—	69.32	—	—	—	—	—
17.6.5	—	69.32	—	—	—	—	—
17.6.4	—	69.32	—	—	—	—	—

Cisco IOS XE Release	NCS4200-1T16G-PS	NCS4200-1T8LR-PS	NCS4200-8T-PS	NCS4200-2Q-P	NCS4200-1H-PK	NCS4200-2H-PQ	NCS4200-1T16LR
17.6.3	—	69.32	—	—	—	—	—
17.6.2	—	69.24	—	—	—	—	—
17.6.1	1.129	1.129	0.21	0.21	0.22	0.2	69.24
17.5.1	1.22	1.22	1.15	0.93	2	0.23	0.2
17.4.1	1.129	69.24	0.21	0.22	0.2	3.4	1.129

Documentation Updates

Rearrangement in the Configuration Guides

- The following are the modifications in the CEM guides.

  Introduction of the OCx CEM Interface Module Configuration Guide. This guide covers the features of the following OCx Interface Modules:

  - 1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module (A900-IMA3G-IMSG)
  - 1-Port OC-192 or 8-Port Low Rate CEM Interface Module (A900-IMA8S1Z-CX)
  - ASR 900 Combo 8-Port SFP GE and 1-Port 10 GE 20G Interface Module (A900-IMA1Z8S-CXMS)
  - 1-port OC-192 or 8-port Low rate CEM interface module

  This features of the OCx interface modules are combined and reorganized as follows:

  - Overview of the interface modules
  - SONET and SDH configuration
  - Interworking Multiservice Gateway (iMSG) that includes serial interfaces, iMSG ACR, multilink interfaces, and VLAN handoff
  - OCx protection that includes Automatic protection switching (APS), Multiplex Section Protection (MSP), Unidirectional Path Switching Ring (UPSR), and Subnetwork Connection Protection (SNCP)
  - Data Communication Channel (DCC) and Target Identifier Address Resolution Protocol (TARP)
  - Bandwidth for OCx Modules

  For more information, see the OCx CEM Interface Module 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)
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)

Supported MIBs		
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

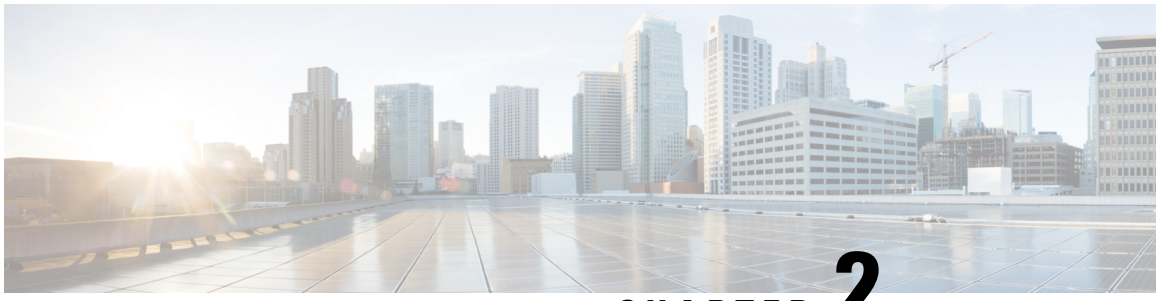
.

- 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

What's New for Cisco IOS XE Bengaluru 17.6.x

This chapter describes the new hardware and software features supported in Cisco IOS XE Bengaluru 17.6.x.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.7

There are no hardware features for this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.7

There are no software features for this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.6a

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.6a

There are no new features in this release. This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see cisco-sa-iosxe-webui-privesc-j22SaA4z.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.6

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.6

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.5

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.5

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.4

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.4

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.3

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.3

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.2

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.2

Feature	Description
T3 or E3 CEM Interface Module	
Channelize the T3 interface into E1 lines	Support for the T3 interface to be channelized into 21 E1 lines.
Quality of Service	
Inter-cos bursting support	This feature introduces color-blind mode of policer operation that is supported on routers with single-rate policer (1R2C) and two-rate policer (2R3C) policing types. With this feature, all policers are supported on color-blind mode with the new template.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.1

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.1

Feature	Description
LAN Switching	
G.8032 Support for IEEE 802.1Q EFPs	This feature supports G.8032 Ethernet ring protection for IEEE 802.1Q Ethernet Flow Points (EFPs). Prior to this release, G.8032 Ethernet ring protection for IEEE 802.1Q was supported only for Trunk Ethernet Flow Points (TEFPs).
High Availability	
Secure eUSB Configuration	Use the **platform secure-cfg** command to provide enhanced security to the routers.
Layer 2	
802.1AE WAN MACsec for 1GE and 10GE NCS4200-1T16G-PS	The WAN MACsec and MKA feature introduce MACsec support on WAN and uplink support and pre-shared key support for the MACsec Key Agreement protocol (MKA). The WAN MACsec supports 1GE and 10GE interfaces for NCS4200-1T16G-PS interface module.

Feature	Description
IP Routing: BFD	
Micro BFD over LAG Convergence Optimization	Starting with 17.6.x release, the convergence for port-channel failures with Fast Reroute (FRR) is less than 50 milliseconds, when min-links is configured and equal to the total-links available under the port-channel. This feature is supported on the Cisco RSP3 module.
First Hop Redundancy Protocols	
Support for BFD, sub-second fast hello for VRRPv3 convergence and re-convergence	This feature supports VRRP failover such that the fault is detected by the VRRP-BFD client within the configured value – when the connection to the remote interface IP address fails. This feature is supported on both the Cisco RSP2 and RSP3 modules.
MPLS Layer 2 VPNs	
Remote LFA for MLDP	Remote Loop-Free Alternate (RLFA) based Fast Reroute (FRR) improves LFA coverage. When used with Multicast Label Distribution Protocol (MLDP) for IPv4, there is no need for an extra protocol in the control plane.
CEM Generic	
Test Access Port (TAP) or Test Access Digroup (TAD)	Support for Test access port or digroup (TAP/TAD) in the following aspects: • Non-intrusive monitoring for both receive and transmit directions. • Split and terminate cross connection for intrusive testing in both directions. The TAP feature helps in monitoring and debugging purpose.
Network Management	
Ingress and Egress Flexible NetFlow	Flexible NetFlow allows you to monitor the traffic from access circuit on an L2VPN and L3VPN network. In addition to monitoring traffic in routed and ethernet service interfaces, you can now monitor traffic in VRF enabled L2 VFI (virtual forwarding interfaces) and cross-connect services. This is only supported on NCS 4206 and NCS 4201/4202 routers.
System Logging	

Feature	Description
Cisco Secure Development Lifecycle—Factory Reset	This feature removes all the customer-specific data that stored on the device since the time of its shipping. Data erased includes configurations, log files, boot variables, core files, and credentials like FIPS-related keys. Cisco Secure Development Lifecycle (CSDL) is a repeatable and measurable proces designed to increse Cisco product resiliency and trustworthiness. The following new commands are introduced: • **factory-reset all** • **factory reset keep-licensing-info** • **factory-reset all secure 3-pass DoD 5220.22-M** For information on the commands, Cisco IOS Configuration Fundamentals Command Reference.
Segment Routing	
IS-IS Flexible Algorithm Include Affinity Support	This feature supports "include-any" and "include-all" affinities in IS-IS. Prior to Cisco IOS XE Bengaluru 17.6.1 release, only Flexible Algorithm affinity "exclude-any" was supported.
OSPF Flexible Algorithm (Ph2): Topology-Independent Loop-Free Alternate (TI-LFA) Path	This feature allows you to configure the Loop-Free Alternate (LFA) and TI-LFA backup or repair paths for a Flexible Algorithm. The backup path is computed based on the constraints and metrics of the primary path. Prior to Cisco IOS XE Bengaluru 17.6.1, OSPF Flexible Algorithm supported only the primary path.
SR-PCE: Enabling SR PM Delay or Liveness for PCE-Initiated Policies	This feature enables the Path Computation Element (PCE) that can provision a Segment Routing Traffic Engineering (SR-TE) policy to mitigate link congestion. Prior to this release, you could only enable PM link and delay measurement using CLI-based policies. Starting with this release, you can also use PCE to enable PM link and delay measurement.
EVPN-IRB DHCP v4 and v6 Relay over Segment Routing	This feature introduces a specialised implementation of DHCP packets to support DHCPv4 and DHCPv6 in an EVPN Fabric with Distributed Anycast Gateways (DAGs) on the same Virtual Routing and Forwarding (VRF). It also avoids DHCP discovery packet floods across the fabric. The flooding suppression feature is also enhanced to intercept multicast or broadcast DHCP packets when DHCP relay is configured on the DAG to perform the required action and localize the scope of the service. This feature is not supported with RSP3 module. It is only supported with RSP2 module. This feature is only supported on NCS 4206 and NCS 4201/4202 routers.

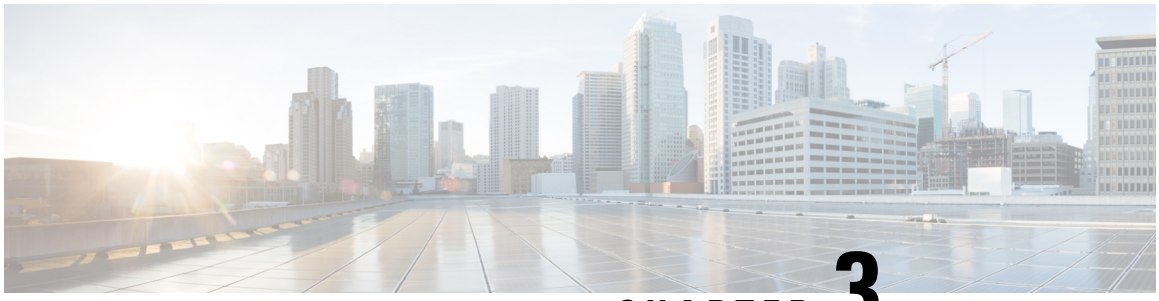
Feature	Description
Stitching of Subnet Route from EVPN to L3VPN	This feature introduces the collpased spine and border leaf node in the network topology of single homing DAGs with symmetric IRB, inter-subnet layer 3 traffic within fabric and inter-subnet layer 3 stitching through layer 3 border gateway. The hosts participating in fabric IRB are directly attached with the collapsed spine and border leaf node. This feature is not supported with the RSP3 module. It is only supported with the RSP2 module. This is only supported on NCS 4206 and NCS 4201/4202 routers.
IP Routing	
Establish GRE Tunnel over VRF Routes	This feature establishes GRE tunnels over Virtual Route Forward (VRF) routes. This feature is not supported with the RSP3 module. It is only supported with the RSP2 module. This is only supported on NCS 4206 and NCS 4201/4202 routers.
Programmability	
FQDN Support for gRPC Subscriptions	With the introduction of the FQDN Support for gRPC Subscriptions feature, along with IP addresses, FQDN can also be used for gRPC subscriptions. Platforms: Cisco Catalyst 9200 Series Switches, Cisco NCS 4200 Series Network Convergence System (RSP2) Cisco Catalyst 9800-40 Series Wireless Controllers, Cisco Catalyst 9800-80 Series Wireless Controllers
YANG Model Support for **show mpls ldp neighbor** Command	This feature enables you to display the status of LDP sessions from YANG models.
YANG Model support for **show mpls tr tunnel** command	This feature enables you to verify the show mpls traffic engineering tunnel command to check the status from YANG models.
YANG Model support for RSVP Commands	You can use the interface BDI 10 and ip rsvp bandwidth percent 4 commands to configure the RSVP bandwidth on a BDI interface from YANG. You can configure, modify and verify different bandwidth values using these commands.
YANG Model support for IPSLA Operating Model for Y1731	You can check the history interval statistics of delay operations like DMM, DMMv1 and 1DM, and loss operations like LMM and SLM using the Netconf-yang command to enable YANG data collection.
YANG Model support for QoS Overhead Accounting	QoS Overhead Accounting feature enables a particular port to consider a particular number of bits that are removed from the packet when the egress packet is re-edited. The traffic scheduler allows more bits than the configured rate at the port, without exceeding the number of bytes that is configured on a port. Yang QOS Overhead accounting configuration model supports the configuration on the router accounting on router from yang/Netconf protocol.

Feature	Description
YANG Model support for alarm profile configurations	This feature enables you to configure the alarm profile on the interface through native YANG models that run on Cisco IOS XE.
YANG Model support for Shared Risk Link Groups (SRLG) Group Identification (GID) configurations	Shared Risk Link Groups (SRLG) Group Identification (GID) configurations can be enabled on YANG using the srlg gid command. Multiple groups and interfaces can be enabled on the interface mode.

YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1761

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.

For more information, see *Programmability Configuration Guide, Cisco IOS XE Bengaluru 17.6.x*.



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 Bengaluru 17.6.7

Identifier	Headline
CSCwh64181	After losing primary master, T-BC stuck in HOLDOVER state though secondary master is reachable.
CSCwh85621	RSP3 : \"sh pla ha cef ip/ipv6\" command is displaying partial output for POCH interface

Open Caveats – Cisco IOS XE Bengaluru 17.6.7

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.6a

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

Open Caveats – Cisco IOS XE Bengaluru 17.6.6a

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.6

Identifier	Headline
CSCwf40403	T3: DCR: cem id not displayed correctly under "sh recovered-clock"
CSCwe38959	rs232 ASYNC PW service with full scale seeing packet and byte drops intermittently
CSCwf40953	DS3_ADMIN_DOWN gets cleared after IM OIR
CSCwe82657	VIN P2/0, VOUT P2/2, VIN P4/0 & VOUT P4/2 alarms upon SSO
CSCwd16666	Ony in 3GMS OC3 port with network loop Bert pattern is not syncing

Identifier	Headline
CSCwf86864	CEM traffic flow is dropped in one direction due to DEI bit set from 4202
CSCwe19162	After SSO: False Alarm on CNAAP
CSCwh02460	with x.21 configured observing underruns in cem counters
CSCwf49426	PAIS alarm get reported after IM OIR.
CSCvy81362	Controllers are down due to LP-LOP alarm After CE reboots
CSCwf07736	cem interface counters momentarily report error when x21 xconnect is cleared and re-established
CSCwe10460	Power sensor threshold warning alarms in EPNM
CSCwf54249	With CPG, STS1e configuration is giving %ERROR: Standby doesn't support this command
CSCwe13024	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
CSCwf71463	with traffic ON, when speed lowered on ASYNC port, SYNC port CEM traffic gets impacted
CSCwe98227	"show version" does not display details of T1/E1 interfaces for 8D and 32D IMs
CSCwf90667	frequent reloads of IM due to high temp- FAN speed mismatch

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.6 - Platform Independent

There are no resolved caveats in this release.

Open Caveats – Cisco IOS XE Bengaluru 17.6.6

Identifier	Headline
CSCwf77316	MPLS L3VPN PE not able to connect remote CE
CSCwd87661	Fan running at high speed and creating noise(Fan PID A903-FAN-H)
CSCwh12668	Standard loopback is not working when applied on both the ends on a back to back link
CSCwh15596	HW Mcirobfd is flapping with Interop tests on RSP3

Open Caveats – Cisco IOS XE Bengaluru 17.6.6 - Platform Independent

Identifier	Headline
CSCvy92900	Crash seen TILFA Flex algo Any cast address during config replace
CSCvy87800	Remote LInk Failure notification is disabled when configuring through YANG
CSCwb43369	Traceback seen when default made on all core intfs.
CSCvy94083	Running configuration syn to the NETCONF running data store takingmor time
CSCuv05226	VRF is not deleted after replacing default config
CSCvy04053	Connect CLI used for local connect needs to take care of monitor session also
CSCvy54819	If show controller cli is executed immediately after l2vpn xconnect config w/o exit, leads to iosd
CSCwd89397	micro bfd: registry call to get encap type of a service instance

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.5

Identifier	Headline
CSCwc41135	Continuous assertion and clear of LAIS on protect channel causing IPC failure
CSCwc80493	APS - K2 byte not reflecting proper value during LRDI and LAIS conditions.
CSCwc25182	Synchronization Status Messaging (S1) Processing and Generation issue
CSCwc41115	APS 1+1 Uni - Tx K2 to reflect Rx K1 channel number
CSCwd04198	A900-IMASER14A/S: when configurations are pasted in a specific order, line config is missing
CSCwd44817	After router reload E1 framing gets changed to unframed in SDH VC12 mode with channe-group config
CSCwd48164	EVPN statd resource leak after protocol flaps
CSCwb90111	17.9 : APS-ACR config/unconfig results in traffic drop
CSCwc34663	FPD: Failure to downgrade the firmware of card 0/0
CSCwd11926	Need support for dual options in CLI for setting clock rate for x21
CSCwb69025	Change in SD-BER threshold value to 10e-9 causes SD alarm assertion

Identifier	Headline
CSCwc65971	RSP3: MPLS pseudowirte - Incorrect label stack pushed to packet
CSCwd60521	ToD state is down with gnss module
CSCwc53354	Alarm assertion/clearing not happening for port x+1 when complete sonet config for port x is removed
CSCwc79322	Memory leak on ptpd_uea process
CSCwd26357	rs485 with half-duplex configuration when reloaded, it gets into default full-duplex mode
CSCwd40870	RSP2 crashes when entering "ip prefix" list

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.5 - Platform Independent

Identifier	Headline
CSCwd66936	RSP2 UDP pseudowire stuck in Activating
CSCwc21402	Invalid BGP update when add-paths negotiated only for label (SAFI 4) and not unicast (SAFI1)
CSCwb91762	RSP3: MSPW VC down points to Error Local access circuit is not ready for label advertise
CSCwb77093	A BGP speaker may advertise a next-hop set to self when advertising an eBGP route to an iBGP peer.

Open Caveats – Cisco IOS XE Bengaluru 17.6.5

Identifier	Headline
CSCwd90840	mcast data traffic is getting dropped over vpls
CSCwd66728	RSP-3C - uea_mgr crash seen with uea_brcm_update_hw_stats
CSCwd87661	Fan running at high speed and creating noise (Fan PID A903-FAN) - SW version 17.03.04
CSCwd16666	Ony in 3GMS OC3 port with network loop Bert pattern is not syncing
CSCwc77502	Unexpected reload due to MLDPv6
CSCwd67723	IOMD Crash and IMA32D/IMA8D card reboot when change E1 config during E1 interface flapping

Identifier	Headline
CSCwd05362	Performance issue on router platform

Open Caveats – Cisco IOS XE Bengaluru 17.6.5 - Platform Independent

Identifier	Headline
CSCwc55520	Traceback and IDB leak noticed when a RSP3 setup performs a switchover
CSCwb43369	Traceback seen when default made on all core intfs
CSCvy94083	Running configuration syn to the NETCONF running data store takes more time
CSCvy87800	Remote Link Failure notification is disabled when configuring through YANG

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.4

Identifier	Headline
CSCwb07758	Convergence is > 50ms during RSP SSO and Core flap with 2 pot-channel interface.
CSCwb60002	ASR900 may experience an unexpected reset when configuring or using interface BDI >= 4097
CSCwb01224	Multihop BFD transit packets getting droppedn on ASR920 after upgrade to 17.3.3
CSCwb46702	MLPPP: Traffic Drop seen after the addition of 2 or more member links
CSCvz91746	ASR903: Tengig interface remained DOWN after ISSU upgrade from 17.04.01 to 17.7.1 throttle
CSCwb33605	Problem with CISCO-ENTITY-SENSOR-MIB SNMP on ASR903 router

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.4 - Platform Independent

Identifier	Headline
CSCwb77396	G.8032: Ring brief output doesnt display the Block port flag in Idle state
CSCwb66047	RSP3/ASR920/RSP2:node crashed @ l2rib_obj_peer_tbl_cmd_print

Open Caveats – Cisco IOS XE Bengaluru 17.6.4

Identifier	Headline
CSCwc34663	FPD: Failure to downgrade the firmware of card 0/0
CSCvz02262	TCAM corruption happening at bank boundary when one of the bank is full.

Open Caveats – Cisco IOS XE Bengaluru 17.6.4 - Platform Independent

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.3

Identifier	Headline
CSCwa99837	RSP3: Implement show command to display voq that failed during delete voq
CSCvy78284	The router will crash when zeroised RSA key is regenerated
CSCwa35351	Raw-socket config-event use all the iomem when L1 is down
CSCvy34396	MAC table inconsistency due to parity error.
CSCvz61352	When IOT IM is inserted in slot 4, gigEth traffic on slot 14 fails
CSCwa09302	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 Exists on System
CSCvz33447	STS1e card protection - Recovered clock status is shown as NA for work and protect ports
CSCwa59045	Need to support few line level CLIs with "no" even without any cable attached.
CSCvz52848	Raw-socket config-event use all the iomem if connected device L1 signals are down
CSCwa79398	rs232 service on port8 gives SLIP errors when databits is set on other ports
CSCwa54842	RSP3: QOSMGR-4-QUEUE_ExCEEDING_HW: VOQs exceeded hardware limit
CSCwb06353	Router crashed with IP SLA configuration which is not supported.
CSCwa94444	F2B chassis: show env does not display the fan speed.

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.3 - Platform Independent

Identifier	Headline
CSCwa37283	RSP failover on router showing several seconds of outage for L2VPN services.

Open Caveats – Cisco IOS XE Bengaluru 17.6.3

Identifier	Headline
CSCvz02262	TCAM corruption happening at bank boundary when one of the bank is full.

Open Caveats – Cisco IOS XE Bengaluru 17.6.3 - Platform Independent

Identifier	Headline
CSCwb04551	FRR is not calculating backup route due to "primary_update_complete_pending:" flag set to 1.
CSCwa30653	MVPN Profile 14: Data MDT traffic not flowing with 2 paths when OSPF cost configured on 1 path.
CSCwa36608	RSP3 ICCP stuck on the CONNECTING state after RSP SO on Active PoA.

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.2

Caveat ID Number	Description
CSCvy08425	With 30 clock ports there are PTP flaps and deselection of current master.
CSCvy51848	Active RP HW goes down during an IO FPGA Upgrade and Standby started booting in Loop.
CSCvy64788	LLC frames are getting looped back due to autonomic networking.
CSCvy74356	In CT3 E1 and CT3 mode, the loopback local is not getting applied, and controller goes down.
CSCvy82376	IMs on slots 13, 14, and 15 out of service on ASR-907 chassis

Caveat ID Number	Description
CSCvy91436	Egress QoS classification issues with Service instance 2 configuration on CE facing interfaces
CSCvz07477	DWDM SFPs threshold Value set to 0.0 dbm for RX/TX and -0.0 C for temperature.
CSCvz19022	Ping issue with MTU greater than 1508.
CSCvz20710	EIGRP flapping on framing SDH Serial interface.
CSCvz26979	DHCP packets are not forwarded from Client to Server when DHCP snooping is enabled globally.
CSCvz57242	IP MTU incorrectly programmed in ASIC after removing/reconfiguring the IP address.
CSCvz79672	HQoS on egress TenGig interface is not working properly.
CSCvz49032	APS ACR scale: traffic goes down after router reload egress counters are 0.
CSCvz37014	Incorrect timestamping: registry to use/update receive timestamp for RSP3 platform.
CSCvz62438	RSP3: BDI routing frames corrupted on deletion and recreation of EFP.
CSCvz09447	IMA1Z8S-CX-MS Protection switching on LOS condition disrupts service for greater than 200 msec.
CSCvz10220	DS3 card protection - iosd crash upon no mode T3.
CSCvz49468	APS:ACR traffic fails after ISSU from 16.12 to 17.3
CSCvz07855	PTP Source port IDs are different in Sync and Announce, Delay-resp packets from the master.
CSCvv65012	Drop tunneled packets for protocols for which tunnel is configured locally.

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.2 - Platform Independent

Caveat ID Number	Description
CSCvz66346	New Bridge-Domain are not added dynamically to POCH when TEFP-encap from-bd is configured.

Open Caveats – Cisco IOS XE Bengaluru 17.6.2

Caveat ID Number	Description
CSCvy78284	The router goes down when zeroised RSA key is regenerated

Caveat ID Number	Description
CSCvz02262	TCAM corruption happening at bank boundary when one of the bank is full.
CSCvz52848	Raw-socket config-event uses all the iomem if connected device L1 signals are down

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.1

Caveat ID Number	Description
CSCvv35215	IP IW XC Scenario - From ethernet to tdm side, IGP label is NOT pushed
CSCvv76949	[SVSP-497]-Op state and Ad state showing NA for all slot with **Bandwidth** command
CSCvz04388	The pubd process crashed during ISSU from 17.6.1 to 17.3_throttle

Open Caveats – Cisco IOS XE Bengaluru 17.6.1

Caveat ID Number	Description
CSCvy74356	In T3 controller-CT3 E1 and CT3 mode the loopback local is not getting applied, controller stays down
CSCvy64388	TAP:Hard IM OIR and router reload causing OBJ_DOWNLOAD_FAIL when multiple modes are enabled

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