![CISCO]

Release Notes for Cisco NCS 4206 and Cisco NCS 4216 Series, Cisco IOS XE Cupertino 17.8.x

First Published: 2022-04-11

C O N T E N T S

C H A P T E R 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.

Cisco NCS 4216 F2B Supported Interface Modules

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

Restrictions and Limitations

Note

The error message "PLATFORM-1-NOSPACE: SD bootflash : no space alarm assert" may occur in the following scenarios:

- Any sector of SD Card gets corrupted

- Improper shut down of router

- power outage.

This issue is observed on platforms which use EXT2 file systems.

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

However, If the error persists after a router reload, we recommend to format the bootflash or FSCK manually from IOS.

- Embedded Packet Capture (EPC) is not supported on NCS 4200 routers.

- From the Cisco IOS XE 16.6.1 releases, In-Service Software Upgrade (ISSU) is not supported on the router to the latest releases. For more information on the compatible release versions, see ISSU Support Matrix.

- ISSU is not supported between a Cisco IOS XE 3S release and the Cisco IOS XE Bengaluru 17.6.x release.

- The port restriction on 1-port OC-192 or 8-port low rate CEM interface module is on port pair groups. If you have OC48 configured on a port, the possible port pair groups are 0–1, 2–3, 4–5, 6–7. If one of the ports within this port group is configured with OC48 rate, the other port cannot be used.

- RS422 pinout works only on ports 0–7.

- The **ip cef accounting** command is *not* supported on the router.

- Configuration sync does *not* happen on the Standby RSP when the active RSP has Cisco Software Licensing configured, and the standby RSP has Smart Licensing configured on the router. If the active RSP has Smart Licensing configured, the state of the standby RSP is undetermined. The state could be pending or authorized as the sync between the RSP modules is not performed.

- Evaluation mode feature licenses may not be available to use after disabling, and enabling the smart licensing on the RSP2 module. A reload of the router is required.

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

Packet Format

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

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

- T1 SAToP, T3 SAToP, and CT3 are supported on an UPSR ring only with local connect mode. Cross-connect configuration of T1, T3, and CT3 circuits to UPSR are not supported.

- PTP is not supported when 8-port 10-Gigabit Ethernet interface module is in oversubscribed mode.

- Port channel 61–64 is not supported in the 16.11.1a release. The range of configurable port channel interfaces has been limited to 60.

- Effective with Cisco IOS XE Everest 16.6.1, the VPLS over Port-channel (PoCH) scale is reduced from 48 to 24 for Cisco ASR 903 RSP3 module.

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

- The frame drops may occur for packets with packet size of less than 100 bytes, when there is a line rate of traffic over all 1G or 10G interfaces available in the system. This restriction is applicable only on RSP2 module, and is not applicable for RSP3 module.

- One Ternary Content-Addressable Memory (TCAM) entry is utilized for Segment Routing Performance Measurement. This is required for the hardware timestamping to function.

- While performing an auto upgrade of ROMMON, only primary partition is upgraded. Use the **upgrade rom-mon filename** command to upgrade the secondary partition of the ROMMON during the auto upgrade. However, the router can be reloaded during the next planned reload to complete the secondary ROMMON upgrade. This is applicable to ASR 903 and ASR 907 routers.

- In the Cisco IOS XE 17.1.1 release, the EVPN EVI type is VLAN-based by default, and while configuring for the EVPN EVI type, it is recommended to configure the EVPN EVI type as VLAN-based, VLAN bundle and VLAN aware model.

- For Cisco IOS XE Gibraltar Release 16.9.5, Cisco IOS XE Gibraltar Release 16.12.3, and Cisco IOS XE Amsterdam 17.1.x, a minimum disk space of 2 MB is required in the boot flash memory file system for a successful ROMMON auto upgrade process. For a disk space lesser than 2 MB, ROMMON auto upgrade fails and the router reboots. This is applicable to Cisco ASR 903 and Cisco ASR 907 routers.

- In the Cisco IOS XE 16.12.1, 17.1.1, and 17.2.1 releases, IPsec is not supported on the Cisco RSP3 module.

- CEM circuit provisioning issues may occur during downgrade from Cisco IOS XE Amsterdam 17.3.1 to any lower versions or during upgrade to Cisco IOS XE Amsterdam 17.3.1 from any lower versions, if the CEM scale values are greater than 10500 APS/UPSR in protected CEM circuits. So, ensure that the CEM scale values are not greater than 10500, during ISSU to or from 17.3.1.

- Some router models are not fully compliant with all IETF guidelines as exemplified by running the pyang tool with the **lint** flag. The errors and warnings that are exhibited by running the pyang tool with the **lint** flag are currently noncritical as they do not impact the semantic of the models or prevent the models

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

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

- Test Access Port (TAP) is not supported when the iMSG VLAN handoff feature is enabled on the same node.

- Data Communication Channel (DCC) is not supported in the NCS4200-1T8S-20CS interface module for the Cisco IOS XE Cupertino 17.8.1 release.

- 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

- In RSP2 and RSP3 modules, during In-Service Software Upgrade (ISSU), interface modules undergo FPGA upgrade.

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

Table 3: Impact on IM during ISSU and FPGA Upgrade

IM	IM Version During ISSU	Pre-ISSU FPGA Upgrade	Post-ISSU Impact on IM	FPGA Version post ISSU
Phase 1	Cisco IOS XE 17.3.x or earlier version to Cisco IOS XE 17.4.x	FPGA upgrade completes and IM starts after the reload process. FPGA version (phase -1) - 0.47	Traffic is impacted during upgrade.	0.75

Phases 1 and 2	Version earlier to Cisco IOS XE 17.8.x	FPGA upgrade completes and IM starts after the reload process.
		- FPGA version (Phase 1)— 0.47
		- FPGA version (Phase 2)
		  - NCS... 62
		  - Combo IM: 69.24
			Traffic is impacted during upgrade.	- FPGA version (Phase 1)—0.75
				- FPGA version (Phase 2)
				  - NCS... 04
				  - Combo IM: 69.32

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

For more information on the FPGA versions, see Supported FPGA Versions.

Refer the following table for supported IMs:

Table 4: NCS 4200 Supported Ethernet Interface Module

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

Determining the Software Version

You can use the following commands to verify your software version:

- Consolidated Package—**show version**
- Individual sub-packages—**show version installed** (lists all installed packages)

Upgrading to a New Software Release

Only the latest consolidated packages can be downloaded from Cisco.com; users who want to run the router using individual subpackages must first download the image from Cisco.com and extract the individual subpackages from the consolidated package.

For information about upgrading to a new software release, see the Upgrading the Software on the Cisco 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	17.8.1	1.22	1.22	1.15	0.93	2.0
CEM FPGA		6	5.2	5G mode: 6.5 10G mode: 7.9	10G mode: 7.0 20G mode: 6.0	9.0
IM FPGA	17.7.1	1.22	1.22	1.15	0.93	2.0
CEM FPGA		0x52110052	0x52520052	5G mode: 0x10090065 10G mode: 0x10070079	10G mode: 0x10290051 20G mode: 0x10290051	0x10030076
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

	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	17.6.1	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
17.8.1	1.129	69.32	0.21	0.21	0.22	0.20	69.24
17.7.1	1.129	1.129	0.21	0.21	0.22	0.20	69.24
17.6.1	1.129	1.129	0.21	0.21	0.22	0.20	69.24
17.5.1	1.22	1.22	1.15	0.93	2.0	0.23	0.20
17.4.1	1.129	69.24	0.21	0.22	0.20	3.4	1.129

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)
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

Supported MIBs		
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 Cupertino 17.8.x

- What's New in Hardware for Cisco IOS XE Cupertino 17.8.1, on page 13
- What's New in Software for Cisco IOS XE Cupertino 17.8.1, on page 13

What's New in Hardware for Cisco IOS XE Cupertino 17.8.1

Feature	Description
Cisco Network Convergence System Routers NCS 4206-16 Series Optics Matrix	
New SFP modules	This release introduces support for the following SFP modules: • ONS-SI+-10G-LR • ONS-SI+-10G-ER • GLC-BX80-D-I—Supported on NCS4200-1T16G-PS

What's New in Software for Cisco IOS XE Cupertino 17.8.1

Feature	Description
Carrier Ethernet	
Latching Loopback	Support the following features for latching loopback on RSP3 module. • Internal and external loopbacks for a port. • Latching loopback states such as prohibited, inactive, and active. • Latching loopback configuration for Connectivity Fault Management (CFM) in both upward and downwards direction on an interface. • Latching loopback activation and deactivation on a service instance

Feature	Description
Support for Number Format in Maintenance Association (MA) Name	This feature supports the MA number format to be passed as an argument to the **service** keyword in the latching loopback **activate** and **deactivate** commands on the RSP3 module. The valid range is from 0 through 65535.
Increase Maximum MTU Size	Maximum Transmission Unit (MTU) is increased to a maximum of 9670 bytes on the Cisco RSP2 module. You can configure the MTU bytes using the **mtu** *bytes* command.
CEM	
CAS feature to perform Super Frame to Extended Super Frame conversion	Channel Associated Signaling (CAS) is a method of signaling each traffic channel rather than having a dedicated signaling channel. CAS uses the same channel, which carries voice or data to pass control signals. This provides an advantage as the implementation of CAS is inexpensive. Supports CAS feature with "in-band" signaling type. You can configure CAS on a specific interface or under global CEM class.
Digital Signaling level zero (DS0) Loopbacks - Network and Local	DS0 loopback is used for testing and troubleshooting the T1 or E1 channel over PSN. You can configure local and remote loopback on channelized T1 or E1 controller (DS0 channel). If the PSN has several NxDS0 pseudowires that are configured at the TDM side, then the same number of NxDS0 loopbacks can be configured on the controller. This provides better TDM maintenance.
Frame Relay Support for IP Interworking	Support for Frame Relay encapsulation on iMSG serial interface for the following interface modules: Frame Relay being a streamlined protocol facilitates higher performance and greater efficiency. • 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 • 1-Port OC-192 or 8-Port Low Rate CEM 20G Bandwidth Interface Module Frame Relay being a streamlined protocol facilitates higher performance and greater efficiency.
IP Multicast: Multicast	
Support of Bidirectional Multicast	Bidirectional PIM or bidirectional multicast (RFC-5015) is an operating mode that enhances PIM by creating bidirectional multicast distribution trees. It helps deploy emerging communication and financial applications that rely on a many-to-many applications model. The following command is introduced: • **ip pim bidir-enable**

Feature	Description
IP Routing: BGP	
Outbound Route Filtering (ORF) Support for BGP Labeled Unicast	This feature uses BGP ORF send and receive capabilities to minimize the number of BGP updates that are sent between BGP peers. It can also filter out unwanted routing updates at the source to reduce the amount of system resources that are required for generating and processing routing updates.
IP SLAs	
Y.1564 and EDPL support on dot1ad	Y.1564 is an Ethernet service activation test methodology and is the standard for turning up, installing, and troubleshooting Ethernet and IP-based services. This methodology allows a complete validation of Ethernet service-level agreements (SLAs) in a single test.
	Ethernet data plane loopback provides a means for remotely testing the throughput of an Ethernet port.
	This feature allows Y.1564 and EDPL to be supported on interfaces configured with 802.1ad encapsulation.
	The following commands are introduced:
	- **inner-eth-type**
	- **outer-eth-type**
Layer 2	
802.1AE WAN MACsec Enhancement for 1GE and 10GE NCS4200-1T16G-PS	The 802.1AE WAN MACsec supports 10GE physical layer (PHY) interfaces for A900-IMA8CS1Z-M interface module. From this release, full HA, Power on Self Test (POST) and double tag support are available on an A900-IMA8CS1Z-M interface module.
	The following command is introduced:
	show-macsec-post
Mac Address Limiting Per Bridge Domain	This feature restricts the number of MAC addresses that the router learns in a bridge-domain on an EFP, pseudowire, or trunk EFP to a specified number. Use the feature to enable warning and limit actions when a violation occurs.
Support for Ethernet Data Plane Loopback on Bundle Interface	This feature enables Ethernet data plane loopback on bundle interfaces. You can also configure the feature when the router is not physically connected and the port is in down state.
	This feature is only applicable on internal or terminal loopback in up or down state.
Maximum Character Limit in Descriptions	The description command in the **l2vpn xconnect** configuration has been modified to support a maximum of 240 characters. In addition, a new description command, which supports 240 characters, has been added in the **connect connection-name** configuration. You can set this by executing the **description** command in the configuration mode. This implementation is useful for administrative purposes.
	The following command is modified:
	• **connect connection-name**

Feature	Description
MPLS: Layer 3 VPNs	
UCMP Load Balancing	The Unequal Cost Multi Path (UCMP) local feature provides the capability to load balance traffic proportionally across multiple paths, with different cost. Prior to this release, the higher bandwidth links used to carry the same traffic as the lower bandwidth links were underutilized. The following command is introduced: • **ucmp local** *prefix-list prefix-list-name*
YANG Model Support for dot1ad Push Operation Under a Service Instance	The **rewrite ingress tag push dot1ad** command pushes the 802.1ad tag on top of the current encapsulation on the ingress packet. Starting from Release 17.8.1, the YANG model supports the push 802.1ad operations on the service instance.
YANG Native Config Model Hardening: Cisco-IOS-XE-wccp.yang	Support for YANG Native Config Model Hardening: Cisco-IOS-XE-wccp.yang.
SE Linux enablement	Support for SE Linux enablement.

C H A P T E R 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 Cupertino 17.8.1

Identifier	Headline
CSCvz62438	ASR90x-RSP3 : BDI routing frames corrupted on deletion and recreation of EFP
CSCwa54842	RSP3: QOSMGR-4-QUEUE_ExCEEDING_HW: VOQs exceeded hardware limit
CSCwa41670	Cylon_mgr crash @adjmgr_get_nh_flag with 16.9.4 image
CSCwa14057	The 'cylon_mgr_F0-0.log' tracelog filling bootflash continuously
CSCvy34396	MAC table inconsistency due to parity error.
CSCvz19022	ASR 903 RSP3C 16.9.3 and 16.12.3 Ping issue with MTU greater than 1508.
CSCvy82376	IMs on slots 13, 14 and 15 out of service on ASR-907 chassis

Identifier	Headline
CSCwa04795	Interfaces are showing up in SNMP polling while associated Hardware Does not Exists on System
CSCvy92074	MTU programming for mpls l2 vc may fail after interface flaps
CSCvz57242	ASR90x-RSP3 : IP MTU wrongly programmed in ASIC after removing/reconfiguring the ip address.
CSCvz49468	APS:ACR traffic fails after ISSU from 16.12 to 17.3
CSCvz79672	HQoS on egress TenGig interface not working properly
CSCvz91746	ASR903: Tengig interface remained DOWN after ISSU upgrade from 17.04.01 to 17.7.1 throttle
CSCvz57514	With scale, APS switch convergence is more than 50 msec.
CSCwa41638	ASR920 MAC Table and L2VPN EVPN Table out of sync
CSCwb06353	Router crashed with IP SLA configuration which is not supported.

Open Caveats – Cisco IOS XE Cupertino 17.8.1

Identifier	Headline
CSCvz02262	TCAM corruption happening at bank boundary when one of the bank is full.
CSCvz65726	Post SSO with QoS OHA counters stops working.

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