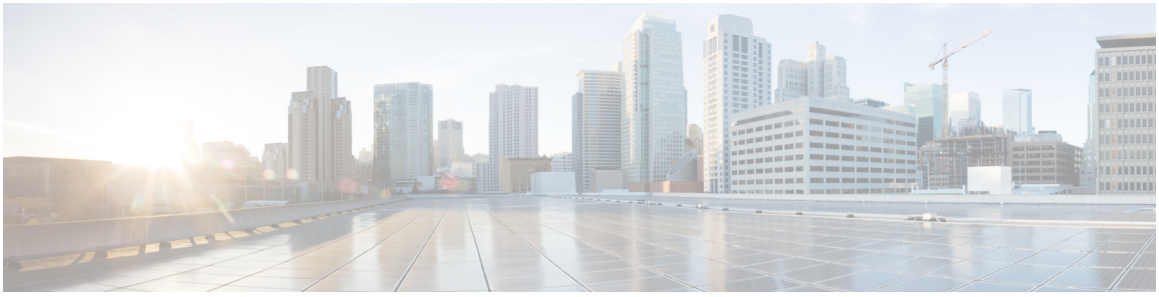
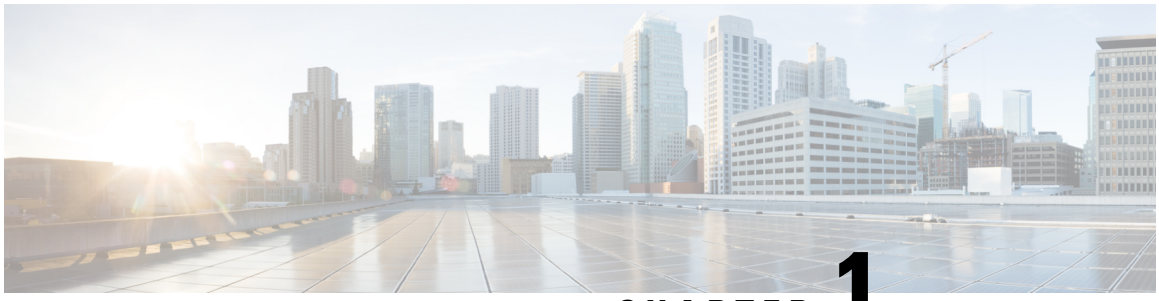
Release Notes for Cisco NCS 4206 and Cisco NCS 4216 Series, Cisco IOS XE Fuji 16.8.x

First Published: 2018-04-16

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.

The Cisco NCS 4206 and Cisco NCS 4216 are full-featured, modular aggregation platforms designed for the cost-effective delivery of converged mobile, residential, and business services.

This document provides information about the IOS XE software release for the Cisco NCS 4206 and Cisco NCS 4216 beginning with 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.

Cisco NCS 4216 F2B

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

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

For more information about the Cisco NCS 4216 F2B Chassis, see the Cisco NCS 4216 F2B Hardware Installation Guide.

NCS 4216 14RU

The Cisco NCS 4216 14RU is a 14-rack unit router that belongs to the Cisco NCS 4200 family of routers. This router complements Cisco's offerings for IP RAN solutions for the GSM, UMTS, LTE, and CDMA. Given its form-factor, interface types and 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-RSP2 Supported Interface Modules

The following table lists the RSP-2 supported interface modules for Cisco NCS 4206 chassis:

RSP Module	Supported Interface Modules	Part Numbers	Slot
NCS420X-RSP-128	SFP Combo IM-8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet Interface Module (1X10GE)	NCS4200-1T8LR-PS	All
	NCS 4200 8X T1/E1 CEM Line Card	NCS4200-8E1T1-CE	All
	1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 ports T1/E1 + 4 ports T3/E3 or 1xOC48 interface over the high-density port	NCS4200-3GMS	All except 0 and 1

Cisco NCS 4206-RSP3 Supported Interface Modules

The following table lists the RSP-3 supported interface modules for Cisco NCS 4206 chassis:

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 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
	1-Port OC192/STM-64 or 8-Port OC3/12/48/STM-1/-4/-16 Interface Module	NCS4200-1T8S-10CS	2,3, 4 and 5
	48 X T1/E1 CEM Interface Module	NCS4200-48T1E1-CE	All
	48 X T3/E3 CEM Interface Module	NCS4200-48T3E3-CE	All
	1-port 10 Gigabit Ethernet (SFP+) / 1-port Gigabit Ethernet (SFP) / 2-port Gigabit Ethernet (CSFP) + 16-port Gigabit Ethernet (CSFP) / 8-port Gigabit Ethernet (SFP) Module.	NCS4200-1T16G-PS	For slot information, see the **Configuring 1-port 10 Gigabit Ethernet (1 X SFP+) / 1-port Gigabit Ethernet (1 X SFP) / 2-port Gigabit Ethernet (1 X CSFP) and 16-port Gigabit Ethernet (8 X CSFP) / 8-port Gigabit Ethernet (8 X SFP)** chapter of the **Cisco NCS 4200 Series Software Configuration Guide**.

Cisco NCS 4216 and Cisco NCS 4216 14RU RSP Supported Interface Modules

The following table lists the RSP supported interface modules for the Cisco NCS 4216 and Cisco NCS 4216 14RU chassis:

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
	1x100G Interface module	NCS4200-1H-PK	7,8
	2x40G Interface module	NCS4200-2Q-P	3,4,7,8,11,12
	8x10G Interface module	NCS4200-8T-PS	3,4,7,8,11,12
	1-Port OC192/STM-64 or 8-Port OC3/12/48/STM-1/-4/-16 Module (10G Mode)	NCS4200-1T8S-10CS	3,4,7,8,11,12
	1-Port OC192/STM-64 or 8-Port OC3/12/48/STM-1/-4/-16 Module (5G Mode)	NCS4200-1T8S-10CS	2,3,4,5,6,7,8,9,10,11,12,13,14,15
	48XT1/E1 Interface module	NCS4200-48T1E1-CE	2,3,4,5,6,7,8,9,10,11,12,13,14,15
	48XT3/E3 Interface module	NCS4200-48T3E3-CE	2,3,4,5,6,7,8,9,10,11,12,13,14,15
	1-port 10 Gigabit Ethernet (SFP+) / 1-port Gigabit Ethernet (SFP) / 2-port Gigabit Ethernet (CSFP) + 16-port Gigabit Ethernet (CSFP) / 8-port Gigabit Ethernet (SFP) Module.	NCS4200-1T16G-PS	For slot information, see the **Configuring 1-port 10 Gigabit Ethernet (1 X SFP+) / 1-port Gigabit Ethernet (1 X SFP) / 2-port Gigabit Ethernet (1 X CSFP) and 16-port Gigabit Ethernet (8 X CSFP) / 8-port Gigabit Ethernet (8 X SFP)** chapter of the **Cisco NCS 4200 Series Software Configuration Guide**.

Restrictions and Limitations for Cisco NCS 4206 and Cisco NCS 4216

- Far end PMON counters are not supported.
- VT PMON is not supported.
- Starting from Cisco IOS XE 16.8.1, M13 framing (channelized and non-channelized) is supported on DS3 IM.

- 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 OCx.
- Port restriction on OCx. If you have OC48 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.
- DS3 over CEP is not supported on DS3 IM.
- 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.
- Traffic is dropped when packets of size 64 to 100 bytes are sent on 1G and 10G ports.
  - For 64-byte packets, traffic drop is seen at 70% and beyond of the line rate.

- For 90-byte packets, traffic drop is seen at 90% and beyond of the line rate.
- For 95-byte packets, traffic drop is seen at 95% and beyond of the line rate.

Traffic is dropped when:

- Traffic is sent on a VRF interface.
- Traffic is sent across layer 2 and layer 3.

However, traffic is not dropped when the packet size is greater than 100 bytes, even if the packets are sent bidirectionally at the line rate.

- 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.

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 Cisco IOS XE 3S consolidated packages can be downloaded from Cisco.com; users who want to run the chassis using individual subpackages must first download the image from Cisco.com and extract the individual subpackages from the consolidated package.

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 1: 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	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	—	—	—	—
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	—	—	—

	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	NCS4200-3GMS	8x10G FPGA	2x40G FPGA	1x100G FPGA
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	—	—	—

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
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)	

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

Unverified MIBs		
ATM-MIB	CISCO-IETF-DHCP-SERVER-EXT-MIB	EXPRESSION-MIB
CISCO-ATM-EXT-MIB		HC-ALARM-MIB
CISCO-ATM-IF-MIB	CISCO-IETF-PPVPN-MPLS-VPN-MIB	HC-RMON-MIB
CISCO-ATM-PVC-MIB	CISCO-IP-STAT-MIB	IEEE8021-CFM-MIB
CISCO-ATM-PVCTRAP-EXTN-MIB	CISCO-IPSLA-ETHERNET-MIB	IEEE8021-CFM-V2-MIB
CISCO-BCP-MIB	CISCO-L2-CONTROL-MIB	IEEE8023-LAG-MIB
CISCO-CALLHOME-MIB	CISCO-LAG-MIB	INT-SERV-GUARANTEED-MIB
CISCO-CIRCUIT-INTERFACE-MIB	CISCO-MAC-NOTIFICATION-MIB	INTEGRATED-SERVICES-MIB
CISCO-CONTEXT-MAPPING-MIB	CISCO-MEMORY-POOL-MIB	MPLS-L3VPN-STD-MIB (RFC 4382)
CISCO-EIGRP-MIB	CISCO-NHRP-EXT-MIB	MPLS-LDP-ATM-STD-MIB (RFC 3815)
CISCO-ERM-MIB	CISCO-NTP-MIB	MPLS-LDP-MIB
CISCO-ETHER-CFM-MIB	CISCO-PING-MIB	MPLS-TE-STD-MIB
CISCO-ETHERLIKE-EXT-MIB	CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB	MPLS-VPN-MIB
CISCO-EVC-MIB	CISCO-RTTMON-ICMP-MIB	NHRP-MIB
CISCO-HSRP-EXT-MIB	CISCO-RTTMON-IP-EXT-MIB	RFC2006-MIB (MIP)
CISCO-HSRP-MIB	CISCO-RTTMON-RTP-MIB	RMON2-MIB (RFC 2021)
CISCO-IETF-ATM2-PVCTRAP-MIB	CISCO-SNMP-TARGET-EXT-MIB	SMON-MIB
CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN	CISCO-TCP-MIB	VRRP-MIB
CISCO-IETF-BFD-MIB	CISCO-VRF-MIB	
CISCO-IETF-DHCP-SERVER-MIB	ETHER-WIS (RFC 3637)	

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:

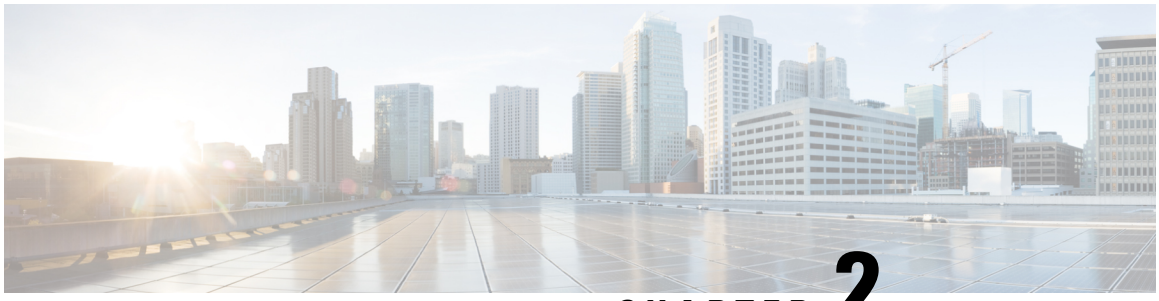
http://www.cisco.com/en/US/products/ps11174/products_licensing_information_listing.html

Communications, Services, and Additional Information

- 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 features supported on the Cisco NCS 4200 Series in this release..

New Software Features for NCS 4206 and NCS 4216 in Cisco IOS XE Fuji 16.8.1b

- **16K EFP Support on Port Channel**

  16K EFPs on port channel are supported.

  For more information, see the Quality of Service Configuration Guidelines, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series).

- **Far-end Performance Monitoring Support**

  The far-end counters for performance monitoring counters are supported for the following interface modules:

  - 48-Port T1/E1 CEM Interface Module
  - 48-Port T3/E3 CEM Interface Module
  - 1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module
  - 1-Port OC-192 or 8-Port Low Rate CEM Interface Module

  The output for the following **show controllers** commands are updated for far-end counters:

  - show controllers t1
  - show controllers e1
  - show controllers t3
  - show controllers e3
  - show controllers sonnet

For more information on performance monitoring, see the

- 48-Port T1/E1 CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)
- 48-Port T3/E3 CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)
- 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, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)
- 1-Port OC-192 or 8-Port Low Rate CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series).

For more information on the updated commands, see the Cisco IOS Interface and Hardware Component Command Reference.

- **Loopback Remote on T1 and T3 Interfaces**

  Loopback remote configuration is suppported. The loopback remote configuration attempts to put the far-end T1 or T3 interfaces into a loopback. The loopback remote setting loops back the far-end at line or payload, using inband bit-orientated CDE (IBOC) or the ESF loopback codes to communicate the request to the far-end. This feature is supported on the following interface modules:

  - 48-Port T1/E1 CEM Interface Module
  - 48-Port T3/E3 CEM Interface Module
  - 1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module
  - 1-Port OC-192 or 8-Port Low Rate CEM Interface Module

  The following new command is introduced for this feature:

  - Loopback remote

  For more information on the loopback remote feature, see the:

  - 48-Port T1/E1 CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)
  - 48-Port T3/E3 CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)
  - 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, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)
  - 1-Port OC-192 or 8-Port Low Rate CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series).

  For more information on the new command, see the Cisco IOS Interface and Hardware Component Command Reference.

- **Multi EFPs for Single BDI Support**

  Multiple EFPs with a single BDI are supported.

For more information, see the Carrier Ethernet Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series).

- **Programmability**
  - Model-Based AAA— Implements the NETCONF Access Control Model (NACM). NACM is a form of role-based access control (RBAC) specified in RFC 6536.
  - NETCONF Global Session Lock and Kill Session—Provides a global lock and the ability to kill non-responsive sessions in NETCONF. During a session conflict or client misuse of the global lock, NETCONF sessions can be monitored via the show netconf-yang sessions command, and non-responsive sessions can be cleared using the clear configuration lock command.
  - NETCONF and RESTCONF Debug commands—Commands for debugging were added.
  - NETCONF and RESTCONF IPv6 Support—Data model interfaces (DMIs) support the use of IPv6 protocol. DMI IPv6 support helps client applications to communicate with services that use IPv6 addresses. External facing interfaces will provide dual-stack support; both IPv4 and IPv6.
  - 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/1681

    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 on the Programmability features, see the Programmability Configuration Guide, Cisco IOS XE Fuji 16.8.x.

- **Support for Alarm Profiling**

  The alarm profiling feature enables you to create a unique alarm profile for chassis, card or interface module, and port. Each alarm profile, for example, chassis alarm profile, is defined with an alarm name. Each alarm profile is classified based on controller types such as SONET, SDH, DS1, and DS3. For each controller type, there are a set of alarms defined with default severity. You can overwrite the default severity using the alarm profile and suppress the syslog facility based on your preference. By default, the syslog facility is enabled for the alarm profile.

  The following new commands are introduced for this feature:

  - alarm-profile
  - alarm-profile attach
  - attach profile-name
  - show alarm-profile

  For more information on the alarm profiling feature, see

  - 48-Port T1/E1 CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)
  - 48-Port T3/E3 CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)
  - 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, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)

- 1-Port OC-192 or 8-Port Low Rate CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series).

For more information on the new commands, see the Cisco IOS Interface and Hardware Component Command Reference.

- **Support of DS1 Framed Structure-Agnostic TDM over Packet (SAToP)**

  Framed Structure-Agnostic TDM over Packet (SAToP) detects an incoming AIS alarm in the DS1 SAToP mode. Framed SAToP helps in the detection of a packet drop and enhances performance by detecting the alarm earlier in the network. This feature is supported on the following interface modules:

  - 48-Port T1/E1 CEM Interface Module
  - 48-Port T3/E3 CEM Interface Module
  - 1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module
  - 1-Port OC-192 or 8-Port Low Rate CEM Interface Module

  Note BERT is not supported in system direction for framed SAToP.

  The **cem-group group-number** command is updated with the new keyword framed as follows:

  - cem-group *group-number framed*

  For more information, see the:

  - 48-Port T1/E1 CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)
  - 48-Port T3/E3 CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)
  - 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, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)
  - 1-Port OC-192 or 8-Port Low Rate CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series).

  For more information on the new command, see the Cisco IOS Interface and Hardware Component Command Reference.

- **Support of DS3 Circuit Emulation over Packet (CEP)**

  DS3 Circuit Emulation over Packet (CEP) feature is introduced to achieve STS-1 or VC4 CEP configuration on the interface module. Here, T3 or E3 can be mapped to either STS-1 or VC4 to be emulated on a packet network.

  This feature is supported on the following interface module:

  - 48-Port T3/E3 CEM Interface Module
  - 1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module

The **show controllers t3** command is updated with the new keyword path as follows:

- show controllers t3 *path*

For more information, see the

- 48-Port T3/E3 CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)
- 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, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series)

For more information on the new command, see the Cisco IOS Interface and Hardware Component Command Reference.

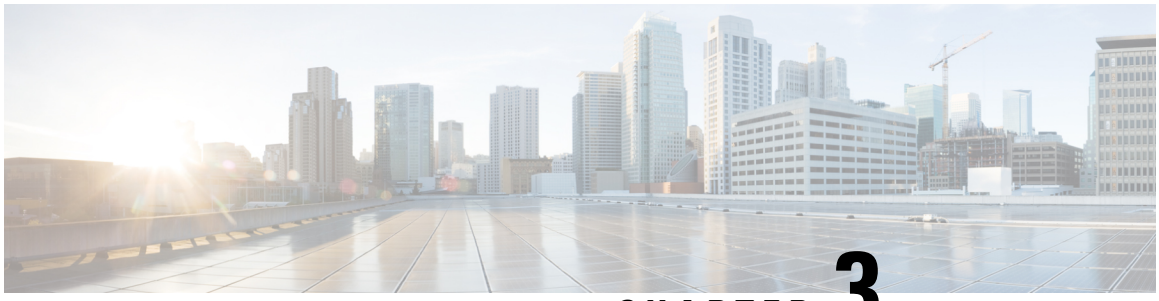
- **VPLS over Backup Pseudowire**

  Pseudowire redundancy allows you to detect any failure in the network and reroute the Layer 2 service to another endpoint that can continue to deliver service by providing additional backup pseudowire. This feature enables recovery from a failure of either the remote provider edge (PE) router or the link between the PE and customer edge (CE) routers.

  For more information, see the MPLS Layer 2 VPNs Configuration Guide, Cisco IOS XE Fuji 16.8.x (Cisco NCS 4200 Series).

New Hardware Features for NCS 4206 and NCS 4216 in Cisco IOS XE Fuji 16.8.1b

There are no new hardware features in this release.



CHAPTER 3

Caveats

This chapter describes open and resolved severity 1 and 2 caveats and select severity 3 caveats:

- The "Open Caveats" sections list open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.
- The "Resolved Caveats" sections list caveats resolved in a specific release, but open in previous releases.

The bug IDs are sorted alphanumerically.

Note The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat you must use the Bug Search Tool.

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

Open Caveats – Cisco IOS XE Fuji 16.8.1b

Caveat ID Number	Description
CSCvb99102	MH BFD session flaps on shutting interface of no relevance to BFD session.
CSCvd50734	RSP3-200:Router Crash while trying to delete label uea_oce_base_delete uea_mpls_label_delete_async
CSCvd58258	IOS-XE display issue show hw-module subslot X/X transceiver X idprom detail

Caveat ID Number	Description
CSCvf79613	Silent crash seen due to machine check exception on IM OIR/RELOAD intermittently
CSCvf96598	RSP2 : ~15sec loss traffic for /HSPW service on ISSU/sso
CSCvg06222	RSP3: ~30sec traffic loss for EOMPLS services during ReOpt after TE Node Protection trigger
CSCvg10313	Cu clock source still squelched on interface bring up after two SSOs
CSCvg23724	QOS fails to secure teleprotection traffic on MLPPP interface
CSCvg84664	Port does not come up with hard loopback inserted
CSCvg98953	1691: UEA_MGR Crash@uea_asic_mpls_lentry_modify seen during stressed soak run
CSCvh07238	Unable to copy image from TFTP to RSP3C bootflash with higher block size
CSCvh15762	RSP3: IOSd Crash in FastPath Thread during Punt Packet Buffer Dequeue on ARP Flaps Soak
CSCvh24638	BDIs static MAC removed after BD shut/no shut while MAC limit is exceeded
CSCvh52708	RSP3: LAG LB is not working based on VC label
CSCvh55399	T1 Service Latency is Asymmetric in a Simple Linear Topology
CSCvh67272	Delay in handing over the packets to UDP in back-to-back setup with IPSLA config/packets.
CSCvh67863	Standby IOMD crash is bringing the active IOMD down with PCIE error
CSCvh79267	RSP3: Hundred gig interface goes down with reload with SR10 H/W settings
CSCvh88811	RSP2 GRE:PIM neighbor ship fails to come up on VRF instance when outgoing interface is BDI
CSCvh90836	Kernel - "Unknown" OBFL crash due to "swapper" task process
CSCvh94635	[RSP3-QOS]:broadcast packets are not being honored by configured policer
CSCvi06300	RSP3: Pending issues seen when converting from Access EFPs to Trunk EFPs
CSCvi06358	Label and outgoing interface programmed wrongly for prefix in RSP3
CSCvi06424	Traffic fails after moving/relearning mac-address from EFP to Xconnect interface
CSCvi11914	BGP PIC/Max-paths:150K scale device stuck with pending issues for huge time with network changes
CSCvi18644	BFD flaps during SSO
CSCvi25777	VID-84-Several Parameter Counters in "sh interfaces gigabitEthernet x/x/x" do not function in 4202

Caveat ID Number	Description
CSCvi34203	RSP2: 10G Controller mode change WAN > LAN triggers LF on Peer resulting port in down state
CSCvi85648	CPAK 100G LR4 optics are not coming up

Resolved Caveats – Cisco IOS XE Fuji 16.8.1b

Caveat ID Number	Description
CSCvc27630	Tx Packets or Tx Bytes generated is always lesser than configured rate-steps
CSCvd13823	Storm control - L3 Mcast Traffic :: Not all packets are dropped
CSCvd38391	Standby Router: uea_mgr crashed @ ml2vpn_provision_pw_and_ac
CSCvd75495	Wrong marking for locally generated packet of BFD, LDP, and BGP
CSCvd87285	Display issue - Egress i/f and L2 stats shows "unknown" and no packet drops
CSCvd89421	RMEP failure due to CFM HW table corruption
CSCve05859	Exxx EIN: G.8275.1 testing: Clock loop forming between synce and ptp
CSCve10095	Traffic is getting dropped in both direction due to hw programming went for toss
CSCve52155	RSP3: BFD Session Between 2 RSP3s Down on Reloading 1 RSP3
CSCve75491	TE auto-bw: Incorrect bandwidth requested on soaking with traffic
CSCvf03157	RSP3:PC stays in suspended state on IM OIR
CSCvf03246	RSP3-CFM : CFM design change to overcome issues with increased MAC add per slot
CSCvf10783	Arbitrary File Overwrite Vulnerability
CSCvf16468	RSP3-QIP: CFM H/w offloaded sessions over xconnect affecting S/w sessions configured over BD
CSCvf21368	RSP3: UEA_Mgr Crash on Checking IPv6 Multicast Flow in the Platform while Flows are Flapping
CSCvf34496	RSP3-QIP:Error objects on Stby cfm_mp_ifh 16794673 sid 3001 download to CPP failed seen upon IM-OIR
CSCvf49124	Management default gateway not reachable with 16.6.1 image
CSCvf55327	CLNS interop with ONS not working
CSCvf60263	APS-ACR Scale Issue:For 8K Scale Config, PW-GROUP not bound on Arrive CEM FPGA during Copy Config

Caveat ID Number	Description
CSCvf64393	After BD MAC limit is exceeded on Trunk EFP Learning gets enabled after adding/removing an encap
CSCvf66442	MPLS IP support over Routed VPLS.
CSCvf68605	DHCP Snooping Database restore/renew failing on all variants
CSCvf69983	Packets not looped back 100% for LLF-external when Responder present in MIP
CSCvf72154	RSP3 - PIM neighborship down on BDI interface due to packets ASIC loop.
CSCvf76449	Observing Object Download Failure on Shut/NO shut with CFM Config
CSCvf77295	MAC limit EXCEED is not received and MAC learning is not disabled after BD shut/no shut
CSCvf79693	RSP3: BGP support over Router PW.
CSCvf80056	MAC-FLAP-Syslog-Not generated for TEFP BDs
CSCvf80724	Complete traffic drop (imp and disp) over VPLS Act PW
CSCvf82589	MPLSoRPW: Traceroute not working over Routed PW interface
CSCvf82663	crashed at dl_callback
CSCvf85222	[RSP3] CFM over PC scale to be reduced to free up 1 Port Scheduler from each ARAD
CSCvf85227	After soak triggers with traffic ipv4 bfd packets take base queue instead on control queue
CSCvf91437	Ping to the loopback IP of remote fails with explicit null configuration.
CSCvf99074	Ping Loss on Built-in Te 0/0/10 or 0/0/11 Port and CRC / MAC Errors at Peer End
CSCvg03308	[RSP3-DHCP-Relay]:unicast dhcp relay is getting dropped in transparent case with HSRP/VRRP/GLBP
CSCvg04717	DDR Busy and Calibration handling in FPGA software driver
CSCvg06788	RSP3:3-10sec traffic loss for FlexLsp Tunnels (unidirectional) from HE to TE on Active path cutover
CSCvg14825	Require varbind entSensorPrecision, Scale and Type along with trap entSensorThresholdNotification
CSCvg21893	Unexpected traffic was sent out from router access port from REP ring
CSCvg21899	Traffic forwarding not happening for VLANs added via "encap dot1q add" command in TEFP
CSCvg23956	RSP2: VPLS Backup PW: Enable member bdi CLI under l2vpn xconnect context
CSCvg26930	Ten Gig interface going into admin down state after one gig shut down

Caveat ID Number	Description
CSCvg28351	VPLS with Segment Routing not flowing traffic.
CSCvg28721	RSP3: uea-mgr crashed while trying to install a label entry in kbp(update case)
CSCvg31959	MLPQ does not work on dynamic modification of queue-limit in higher priority level class.
CSCvg35782	MPLSoRPW: Console msg "RPW's exceeded supported limit 128"
CSCvg36200	IPv4 deny ACL applied in the BDI is blocking L2 switched traffic under certain conditions
CSCvg36419	LLF internal in RSP2 is not working properly
CSCvg42691	RSP3- P node ECMP loadbalancing failing for ip traffic
CSCvg43975	RSP3: Leak in G8032 IOS TDL Messaging on Flapping the Ring
CSCvg44405	WRT : storm-control unable to fetch correct level in percentage value, hence failing to take action
CSCvg48485	RSP3 - Ingress LDP label incorrectly programmed to FEC 0x0
CSCvg53410	RSP3: IMA1X handle PHY HiBER events
CSCvg53877	Egress QOS Fails when speed is changed at interface via nego auto, speed cli command
CSCvg63915	2 Xconnect TDL Messages Leaked in Cylon_Mgr on "show running-config"
CSCvg70409	IOT: For Serial IM, flowcontrol is not applicable
CSCvg74427	fan tray external alarm input should not cause RSP to crash
CSCvg79798	"ZTP reset" as last reload reason in IOS when ZTP button pressed > 8sec
CSCvg83081	Fixed Ports moving to admin down state after IMA8S insertion
CSCvg84699	BFD session not coming up on RSP3 due to wrong platform offload limit
CSCvg85163	ZTP not triggered with Gratuitous ARP
CSCvg88049	Remove IOS syslog message for link status IDLE
CSCvg91082	1681: Crash@uea_brcm_vfi_notify_bdi_state_change seen during stressed soak run
CSCvg93982	IOS XE entSensorThresholdNotification trap is not generated for Card Temperature
CSCvh03346	Fan speed display in IOS not matching the actual written value and read value
CSCvh06736	Device crashes on dynamically attaching a class to a policy .
CSCvh08220	RSP3: Crash in IOSD chasfs task on Defaulting and Removing IMA-1X
CSCvh10730	BFD stuck at init state for Sessin ID 1023 alone on RSP3C after link flap

Caveat ID Number	Description
CSCvh20282	Traffic is not flooding on all the interface for same TEFP BD
CSCvh68935	RSP3/RSP2: BFD Flap on the link between RSP3 (8x10G) and RSP2 (Combo 10G) with switchover
CSCvh83722	All BFD Sessions Down as FPGA Stuck due to invalid Packet Length and Offset Error in DDR3
CSCvi06424	Traffic fails after moving/relearning mac-address from EFP to Xconnect interface