Release Notes for Cisco NCS 4206 and Cisco NCS 4216 Series, Cisco IOS XE 3.18SP

First Published: 2016-07-29

Last Modified: 2020-07-10

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

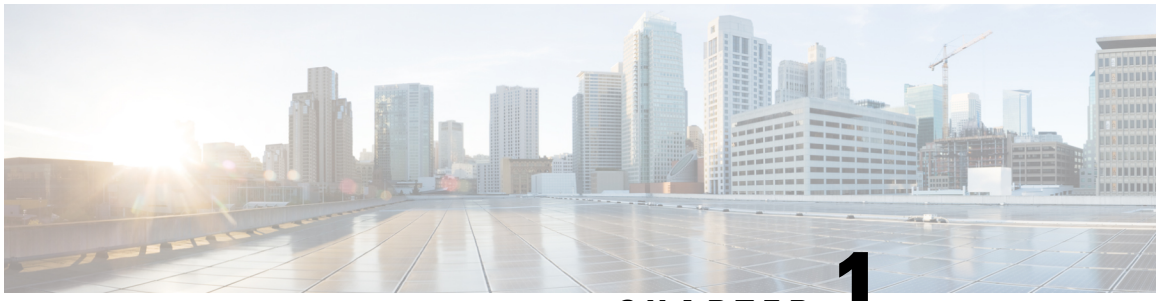
Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2016–2020 Cisco Systems, Inc. All rights reserved.

CONTENTS



CHAPTER 1

Introduction

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 Cisco IOS XE Everest 16.5.1, which is the first supported release in the Release 16 Series.

Introduction

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 Cisco IOS XE Everest 16.5.1, which is the first supported release in the Release 16 Series.

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.

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

The following table lists the 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
	OC-192 Interface module + 8-port Low Rate 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

Cisco NCS 4216 RSP Supported Interface Modules

The following table lists the RSP supported interface modules for Cisco NCS 4216 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
	OC-192 Interface Module with 8-port Low Rate CEM Interface Module (10G HO / 10G LO)	NCS4200-1T8S-10CS	3, 4, 7, 8, 11, 12
	OC-192 Interface Module with 8-port Low Rate CEM Interface Module (5G HO / 5G LO)	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

Restrictions and Limitations for Cisco NCS 4206 and Cisco NCS 4216

- Far end PMON counters are not supported.
- VT PMON is not supported.
- M13 framing is not 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.
- 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.

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 and ROMmon Versions

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.

From Cisco IOS XE Release 3.18SP onwards, the minimum recommended ROMmon version is 15.6(12r)S.

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 and ROMmon Versions

	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	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	3.18.8aSP	1.22	1.22	1.15	0.17	—	—
CEM FPGA		0x46240046	0x46240046	0x10690070	—	—	—

	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	8x10G FPGA	2x40G FPGA	1x100G FPGA
IM FPGA	3.18.9SP	1.22	1.22	1.15	0.21	0.22	0.19
CEM FPGA		0x46240046	0x46240046	0x10690070	—	—	—
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	—	—	—

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)

Supported MIBs		
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:

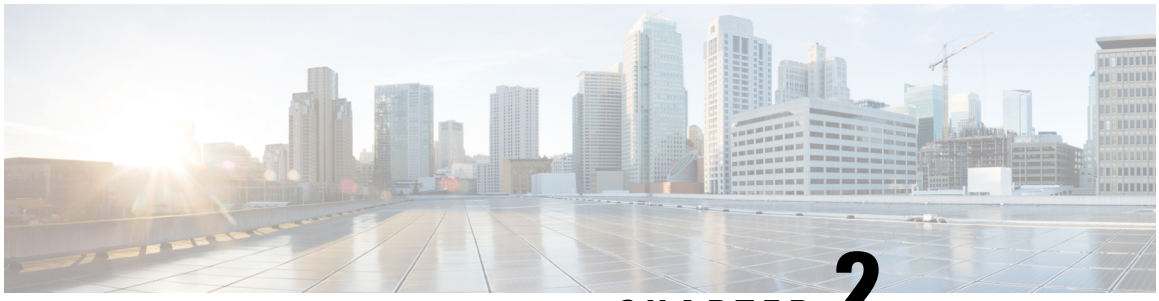
http://www.cisco.com/en/US/products/ps11174/products_licensing_information_listing.html

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 in Cisco IOS XE Release 3.18.9SP

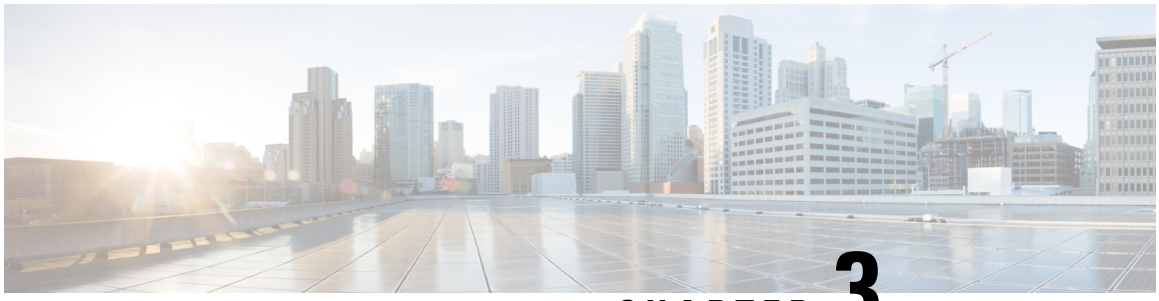
This chapter describes the new features supported on the Cisco NCS 4200 Series.

New Hardware Features in Cisco IOS XE Release 3.18.9SP

There are no new hardware features in the Cisco IOS XE Release 3.18.9SP.

New Software Features in Cisco IOS XE Release 3.18.9SP

There are no new software features in the Cisco IOS XE Release 3.18.9SP.



CHAPTER 3

New Features in Cisco IOS XE Release 3.18.8aSP

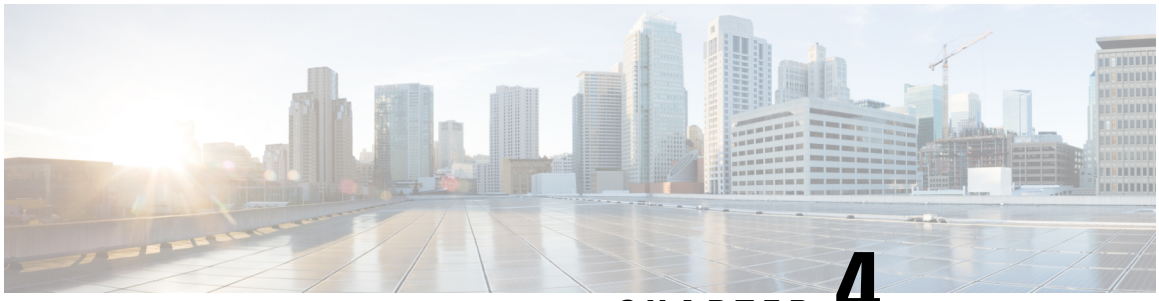
This chapter describes the new features supported on the Cisco NCS 4200 Series.

New Software Features in Cisco IOS XE Release 3.18.8aSP

There are no new software features in the Cisco IOS XE Release 3.18.8aSP.

New Hardware Features in Cisco IOS XE Release 3.18.8aSP

There are no new software features in the Cisco IOS XE Release 3.18.8aSP.



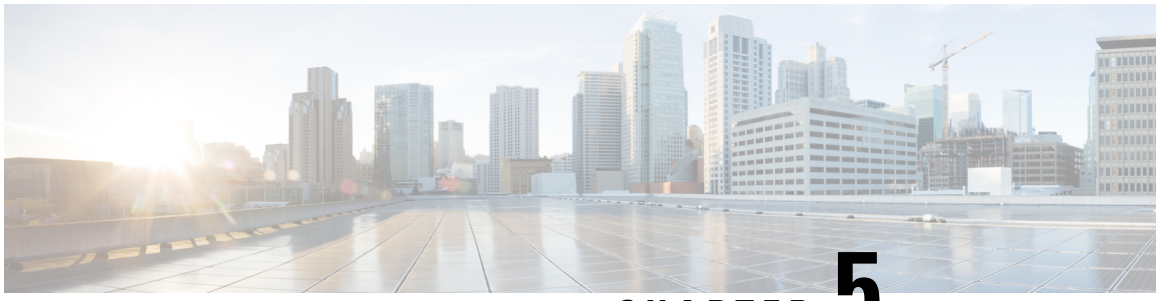
CHAPTER 4

New Features in Cisco IOS XE Release 3.18.7SP

This chapter describes the new features supported on the Cisco NCS 4200 Series.

New Hardware Features in Cisco IOS XE Release 3.18.7SP

There are no new hardware features in the Cisco IOS XE Release 3.18.7SP.



CHAPTER 5

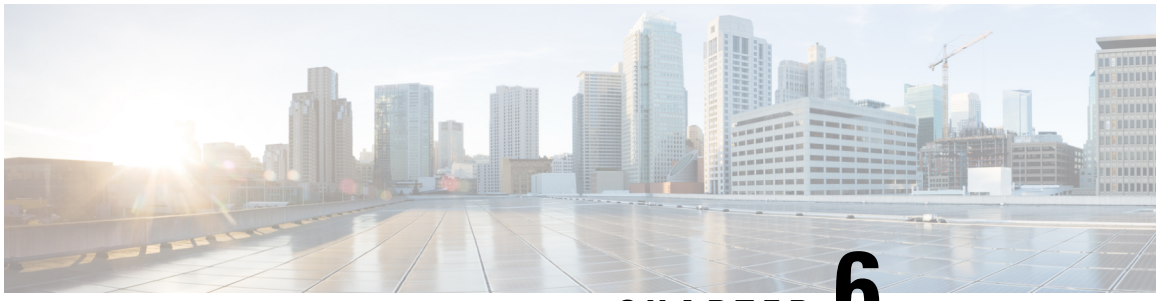
New Software Features in Cisco IOS XE Release 3.18.7SP

There are no new software features in the Cisco IOS XE Release 3.18.7SP.

• New Hardware Features in Cisco IOS XE Release 3.18.7SP, on page 17

New Hardware Features in Cisco IOS XE Release 3.18.7SP

There are no new hardware features in the Cisco IOS XE Release 3.18.7SP.



CHAPTER 6

New Features in Cisco IOS XE Release 3.18.6SP

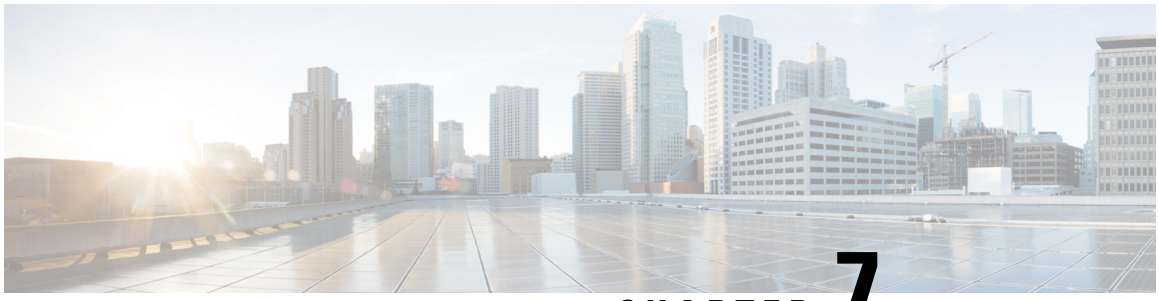
This chapter describes the new features supported on the Cisco NCS 4200 Series.

New Software Features in Cisco IOS XE Release 3.18.6SP

There are no new software features in the Cisco IOS XE Release 3.18.6SP.

New Hardware Features in Cisco IOS XE Release 3.18.6SP

There are no new hardware features in the Cisco IOS XE Release 3.18.6SP.



CHAPTER 7

New Features in Cisco IOS XE Release 3.18.5SP

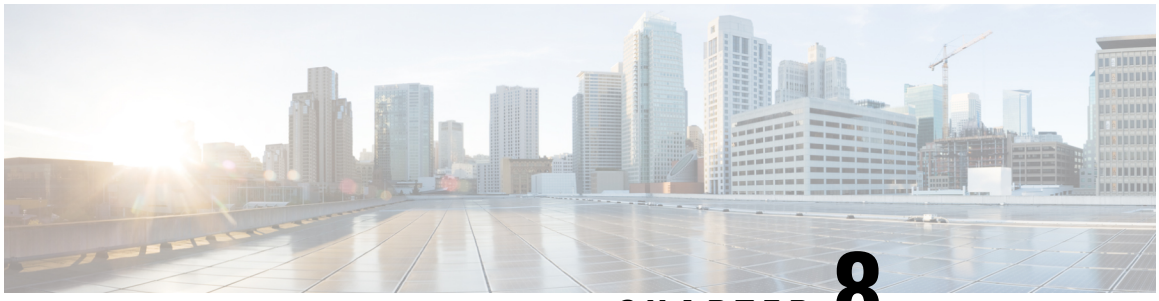
This chapter describes the new features supported on the Cisco NCS 4200 Series.

New Software Features in Cisco IOS XE Release 3.18.5SP

There are no new software features in the Cisco IOS XE Release 3.18.5SP.

New Hardware Features in Cisco IOS XE Release 3.18.5SP

There are no new hardware features in the Cisco IOS XE Release 3.18.5SP.



CHAPTER 8

New Features in Cisco IOS XE Release 3.18.4SP

This chapter describes the new features supported on the Cisco NCS 4200 Series.

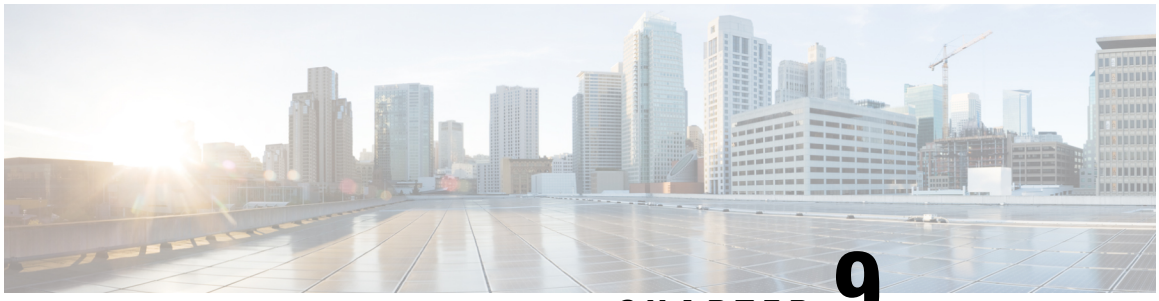
New Hardware Features in Cisco IOS XE Release 3.18.4SP

There are no new hardware features in the Cisco IOS XE Release 3.18.4SP.

New Software Features in Cisco IOS XE Release 3.18.4SP

Multi EFPs for Single BDI Support on Cisco RSP3 Module

The Cisco RSP3 module now supports multiple EFPs with a single BDI.



CHAPTER 9

New Features in Cisco IOS XE Release 3.18.3SP

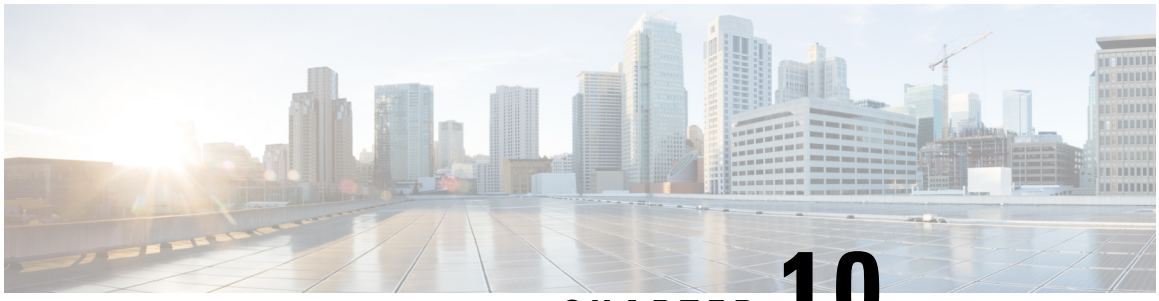
This chapter describes the new features supported on the Cisco NCS 4200 Series.

New Hardware Features in Cisco IOS XE Release 3.18.3SP

There are no new hardware features in the Cisco IOS XE Release 3.18.3SP.

New Software Features in Cisco IOS XE Release 3.18.3SP

There are no new software features in the Cisco IOS XE Release 3.18.3SP.



CHAPTER 10

New Features in Cisco IOS XE Release 3.18.1SP

This chapter describes the new features supported on the Cisco NCS 4200 Series with Cisco IOS XE Release 3.18.1SP.

- New Hardware Features in Cisco IOS XE Release 3.18.1SP, on page 27
- New Software Features in Cisco IOS XE Release 3.18.1SP, on page 27

New Hardware Features in Cisco IOS XE Release 3.18.1SP

There are no new hardware features in the Cisco IOS XE Release 3.18.1SP.

New Hardware Features in Cisco IOS XE Release 3.18.1cSP

There are no new hardware features in the Cisco IOS XE Release 3.18.1cSP.

New Software Features in Cisco IOS XE Release 3.18.1SP

- FlexLSP Inter-area support on non co-routed mode

  Flex LSP supports inter-area tunnels with non co-routed mode. For more information on the restrictions for this feature and its configuration details, see MPLS Basic Configuration Guide for Cisco NCS 4200 Series.

- Leap Second

  Starting with Cisco IOS-XE Release 3.18.1SP, you can configure the leap second event date and Offset value (+1 or -1) on master ordinary clock, hybrid boundary clock, dynamic ports, and virtual ports. The following two new keywords are added to the **utc-offset** command:

  - **leap-second**
  - **offset**

  You can also configure time properties holdover time on boundary clock, hybrid boundary clock, and dynamic ports. The following new command is introduced:

  - **time-properties persist**

For more information, see Cisco NCS 4200 Series Software Configuration Guide.

For more information, see Cisco IOS Interface and Hardware Component Command Reference.

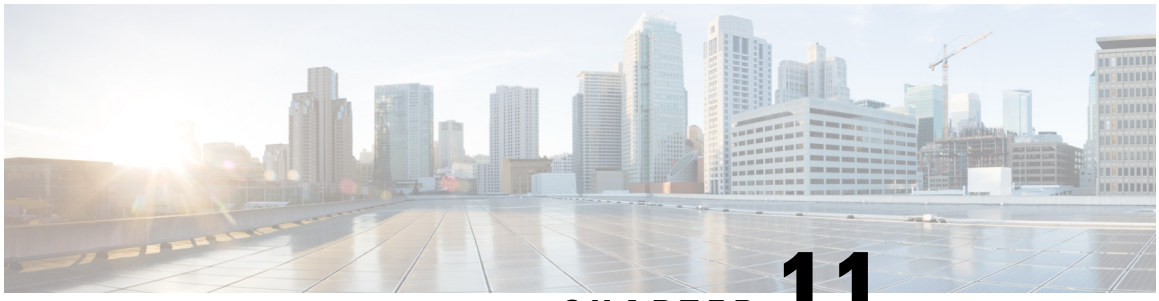
- WAN-PHY Support

  Effective Cisco IOS XE 3.18.1SP, A900-IMA8Z Interface Modules support LAN/WAN-PHY mode.

  For more information, see Cisco NCS 4200 Series Software Configuration Guide.

New Software Features in Cisco IOS XE Release 3.18.1cSP

There are no new software features in the Cisco IOS XE Release 3.18.1cSP.



CHAPTER 11

New Features in Cisco IOS XE Release 3.18SP

This chapter describes the new features supported on the Cisco NCS 4200 Series.

New Software Features in Cisco IOS XE Release 3.18SP

- ACR and DCR Support

  Adaptive Clock Recovery (ACR) is an averaging process that negates the effect of random packet delay variation and captures the average rate of transmission of the original bit stream. ACR recovers the original clock for a synchronous data stream from the actual payload of the data stream.

  Differential Clock Recovery (DCR) is a technique used for Circuit Emulation (CES) to recover clocks based on the difference between PE clocks. TDM clock frequency is tuned to receive differential timing messages from sending end to the receiving end.

  ACR and DCR configuration is supported on 48xT3E3 and 48xT1E1 interface modules.

  For more information on 48xT3/E3 CEM Interface Module, see Configuring 48xT3/E3 CEM Interface Module.

  For more information on 48xT1/E1 CEM Interface Module, see Configuring 48xT1/E1 CEM Interface Module.

- Alarm History

  Alarm history or alarm persistence feature enables the maintenance of the history of the port and the path alarms of the following interface modules:

  - NCS4200-48T3E3-CE
  - NCS4200-48T1E1-CE
  - NCS4200-1T8S-10CS

  History of the port-level and path-level alarms are saved into a file and is retained for monitoring network events.

  For more information, see Alarm History .

- APS support on 1X OC-192 and 8X OC-48 Interface Modules

Automatic protection switching (APS) is a protection mechanism for SONET networks that enables SONET connections to switch to another SONET circuit when a circuit failure occurs. A protection interface serves as the backup interface for the working interface. When the working interface fails, the protection interface quickly assumes its traffic load. 1X OC-192 and 8X OC-48 Interface Modules supports the following SONET protection switching schemes:

- Linear Bidirectional 1+1 APS
- Linear Unidirectional 1+1 APS

For more information, see Configuring SONET on 1X OC-192 and 8X OC-48 Interface Modules.

- Circuit Emulation Support on 48xT1/E1 IM, 48xT3/E3 IM, and 1x OC-192 or 8-port Low Rate CEM Interface Module (10G HO / 10G LO)

  Circuit Emulation (CEM) is a technology that provides a protocol-independent transport over a packet-based backhaul technology such as MPLS or IP Networks. CEM provides a bridge between a time-division multiplexing (TDM) network and MPLS network. L2VPN over IP/MPLS is also supported on the interface modules.

  Note
  - For OC-192 interface module, 1G interface is not supported in Cisco IOS XE Release 3.18SP.
  - CEM is supported only on Cisco NCS 4206 and Cisco NCS 4216.

  For more information on 48xT1/E1 CEM Interface Module, see Configuring 48xT1/E1 CEM Interface Module.

  For more information on 48xT3/E3 CEM Interface Module, see Configuring 48xT3/E3 CEM Interface Module.

  For more information on 1x OC-192 or 8-port Low Rate CEM Interface Module, see Configuring CEM on 1x OC-192 or 8-port Low Rate CEM Interface Module (10G HO / 10G LO).

- DS1 support on 48 ports T1/E1 Interface Module

  This release introduces the DS1 support on 48 ports T1/E1 Interface Module. The 48xT1/E1 with circuit emulation line card supports generic single or dual-port T1 trunk interfaces for voice, data, and integrated voice or data applications.

  Note
  - In Cisco IOS XE Release 3.18SP, E1 is not supported.
  - T1 is supported only on Cisco NCS 4206 and Cisco NCS 4216.

  For more information, see Configuring 48xT1/E1 CEM Interface Module.

- DS3 Channelization Support

  A channelized interface is an interface that is a subdivision of a larger interface. Channelization minimizes the number of physical interface modules and enables users with different access speeds and bandwidth. DS3 Channelization supports each port on a T3 interface to channelize up to 28T1 channels.

For more information, see Configuring 48xT3/E3 CEM Interface Module.

- DS3 support on 48 ports T3 Interface Module

  This release introduces the DS3 support on 48 ports T3 Interface Module. The 48xT3/E3 with circuit emulation line card supports 48 ports. The channels on the T3 interfaces can be configured as either clear channel mode or channelized mode.

  Note
  - In Cisco IOS XE Release 3.18SP, E3 is not supported.
  - T3 is supported only on Cisco NCS 4206 and Cisco NCS 4216.

  For more information, see Configuring 48xT3/E3 CEM Interface Module.

- Loopback and BERT Support

  Loopback tests allow you to isolate pieces of the circuit and test them separately, when a serial line does not come up as it must.

  Bit Error Rate Test (BERT) checks communication between the local and the remote ports. BER tests allow you to test cables and diagnose signal problems in the field. The BERT patterns are supported on channelized line cards to test more thoroughly for bit errors.

  For more information on 48xT1/E1 CEM Interface Module, see Configuring 48xT1/E1 CEM Interface Module.

  For more information on 48xT3/E3 CEM Interface Module, see Configuring 48xT3/E3 CEM Interface Module.

- Maintenance Data Link Support

  Maintenance Data Link (MDL) supports to send messages to communicate identification information between the local and remote ports.

  The MDL message includes:

  - Equipment Identification Code (EIC)
  - Location Identification Code (LIC)
  - Frame Identification Code (FIC)
  - Unit
  - Path Facility Identification (PFI)
  - Port Number
  - Generator Identification Number

  For more information, see Configuring 48xT3/E3 CEM Interface Module.

- OC3/OC12 Smart SFP supporting CEP

  The OC3/OC12 Smart SFP supporting CEP (VCoP Smart SFP) is a special type of optical transceiver which encapsulates SONET bit stream at STS1 or STS-3c or STS-12c level into packet format. The VCoP Smart SFP forwards the SONET signal fully transparently.

Note OC3/OC12 Smart SFP feature is supported only on Cisco NCS 4201 and Cisco NCS 4202.

For more information, see Configuring VCoP Smart SFP.

- ONS pluggable optics support on 1X OC-192 and 8X OC-48 Interface Modules

  Cisco NCS 4200 offers a comprehensive range of pluggable optical modules.

  For more information, see Configuring SONET on 1X OC-192 and 8X OC-48 Interface Modules.

- OTN Wrapper

  Optical Transport Network (OTN) Wrapper feature provides robust transport services that leverage many of the benefits such as resiliency and performance monitoring, while adding enhanced multi-rate capabilities in support of packet traffic, plus the transparency required by Dense Wavelength Division Multiplexing (DWDM) networks. Cisco NCS 4200 acts as an aggregator for ethernet, TDM, and SONET traffic to connect to an OTN network and vice versa. The ports on the interface modules are capable of OTN functionality.

  The OTN Wrapper feature is supported on the following interface modules:

  - 8x10GE (NCS4200-8T-PS)—The encapsulation type is OTU1e and OTU2e.
  - 2x40GE (NCS4200-2Q-P)—The encapsulation type is OTU3.

  For more information, see OTN Wrapper Overview.

- Performance Monitoring

  Performance monitoring (PM) parameters are used by service providers to gather, store, and set thresholds, and to report performance data for early detection of problems.

  For more information, see Configuring SONET on 1X OC-192 and 8X OC-48 Interface Modules.

- QoS support on CEMoMPLS

  The QoS EXP Matching feature allows you to classify and mark network traffic by modifying the Multiprotocol Label Switching (MPLS) experimental bits (EXP) field in IP packets. This feature allows you to organize network traffic by setting values for the MPLS EXP field in MPLS packets. By choosing different values for the MPLS EXP field, you can mark packets so that packets have the priority that they require during periods of congestion.

  For more information, see CEM over MPLS QOS.

- SONET support on 1X OC-192 and 8X OC-48 Interface Modules

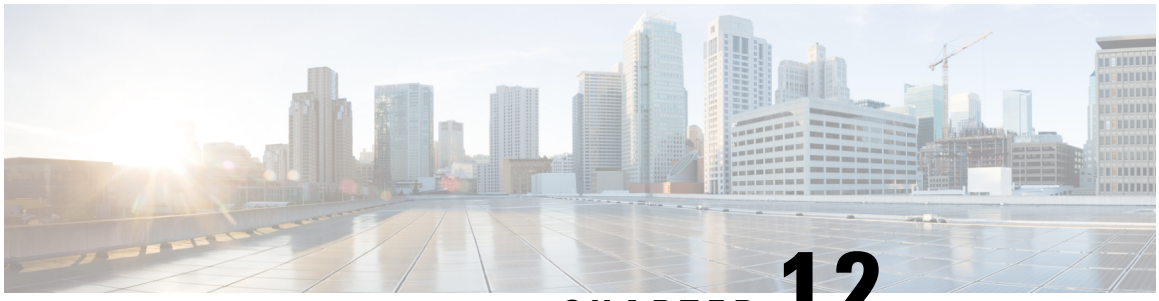
  Synchronous Optical NETwork (SONET) defines optical signals and a synchronous frame structure for multiplexed digital traffic. SONET is supported on 1X OC-192 and 8X OC-48 interface modules. The transport network using SONET provides much more powerful networking capabilities than existing asynchronous systems. SONET is a set of standards that define the rates and formats for optical networks specified in GR-253-CORE.

  For more information, see Configuring SONET on 1X OC-192 and 8X OC-48 Interface Modules .

New Hardware Features in Cisco IOS XE Release 3.18SP

The following Interface Modules were introduced:

- 48 X T1/E1 CEM Interface Module—The 48 X T1/E1 interface module provides connectivity for up to 48 x T1/E1 ports through 3 high-density connectors on the front panel. Each port supports 16 TX and RX ports.
- 48 X T3/E3 CEM Interface Module—The 48 X T3/E3 interface module provides connectivity for up to 48 x T3/E3 ports through 3 high-density connectors on the front panel. Each port supports 16 TX and RX ports.
- OC-192 Interface Module with 8-port Low Rate CEM Interface Module (10G HO / 10G LO)—The OC-192 interface module with 8-port low rate CEM interface module is a high density combination interface module. This module supports 1 OC-192 port and 8 low rate CEM or 1 Gigabit Ethernet port.



CHAPTER 12

Caveats in Cisco IOS XE Release 3.18.9SP

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

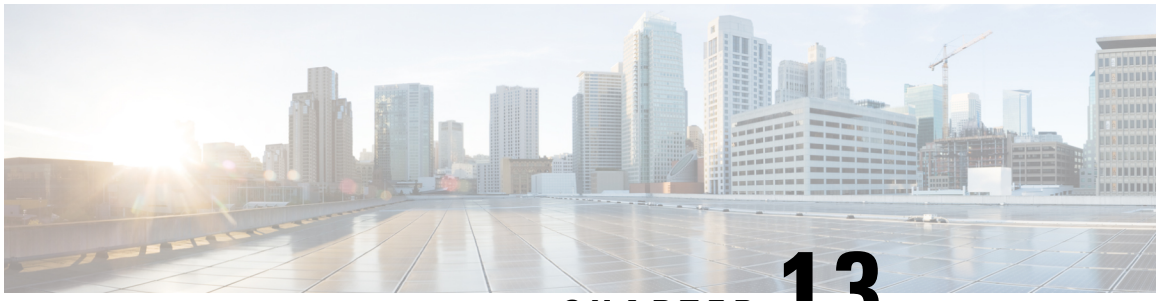
Cisco Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve effectiveness in network risk management and device troubleshooting. You can search for bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. For more details on the tool, see the help page located at http://www.cisco.com/web/applicat/cbsshelp/help.html

Open Caveats – Cisco IOS XE Release 3.18.9SP

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE Release 3.18.9SP

Caveat ID Number	Description
CSCvu78801	PPPoE VSA tags get overwritten at each PPPoE IA



CHAPTER 13

Caveats in Cisco IOS XE Release 3.18.8aSP

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 Release 3.18.8aSP

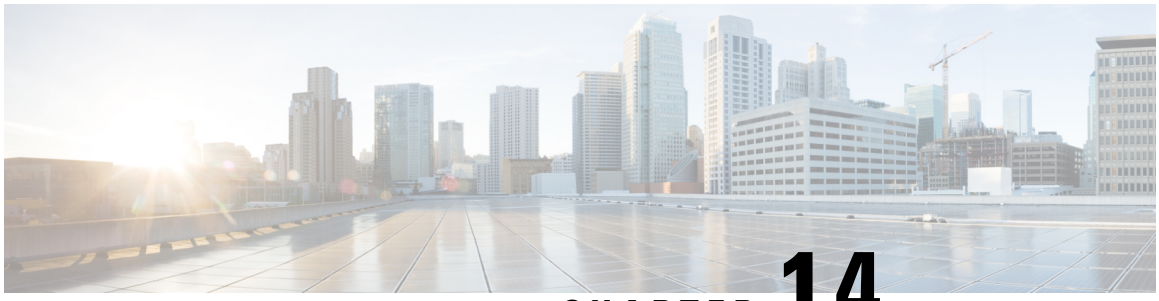
Caveat ID Number	Description
CSCva43417	E1 Interfaces go DOWN on remote alarm (RDI)
CSCvm76770	Unpredictable asymmetry on T1 or E1 interface module

Resolved Caveats – Cisco IOS XE Release 3.18.8aSP

Caveat ID Number	Description
CSCvi02398	SNMP MIB and device configurations do not match

Resolved Caveats – Cisco IOS XE Release 3.18.8aSP Platform Independent

Caveat ID Number	Description
CSCvm79556	RSP3: MSPW VC down after Switchover (Error Local access circuit is not ready for label advertise)
CSCvj15469	Remove crypto group access check



CHAPTER 14

Caveats in Cisco IOS XE Release 3.18.7SP

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 Release 3.18.7SP

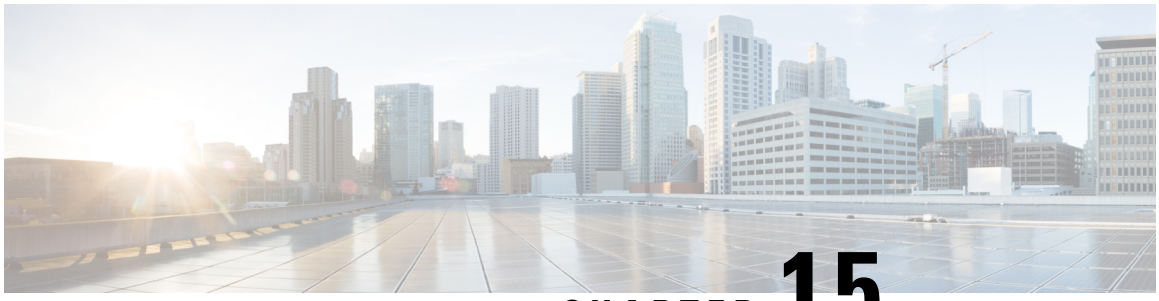
Caveat ID Number	Description
CSCva43417	E1 Interfaces go DOWN on remote alarm (RDI)
CSCvm76770	Unpredictable asymmetry on T1 or E1 interface module

Resolved Caveats – Cisco IOS XE Release 3.18.7SP

Caveat ID Number	Description
CSCvj75078	RSP3: IOMD crash @ iomd_bsess_open_callback_retry on new active after RP SSO
CSCvj87085	PTPD crashed after removing the ptp configs, default profile <169>
CSCvk32423	IMA8Z 6-port mode, hwidx not created leading to complete traffic drop
CSCvm04696	Mac learnt on G8032 blocked ports due to DHCPv4 discovery pkts
CSCvo58053	High memory usage only on standby RSP in iomd
CSCvo65688	TOD flaps in router (master) when setup is left overnight
CSCvp67025	RSP2: Software-Induced Multi-Bit Errors on Handoff FPGA When Exceeding Max FNF Cache Size
CSCvq55841	With netflow enabled, FPGA_INTERRUPTS_ERROR observed upon modifying the flow count

Resolved Caveats – Cisco IOS XE Release 3.18.7SP

Caveat ID Number	Description
CSCvj75078	RSP3: IOMD crash @ iomd_bsess_open_callback_retry on new active after RP SSO
CSCvj87085	PTPD crashed after removing the ptp configs, default profile <169>
CSCvk32423	IMA8Z 6-port mode, hwidx not created leading to complete traffic drop
CSCvm04696	Mac learnt on G8032 blocked ports due to DHCPv4 discovery pkts
CSCvo58053	High memory usage only on standby RSP in iomd
CSCvo65688	TOD flaps in router (master) when setup is left overnight
CSCvp67025	RSP2: Software-Induced Multi-Bit Errors on Handoff FPGA When Exceeding Max FNF Cache Size
CSCvq55841	With netflow enabled, FPGA_INTERRUPTS_ERROR observed upon modifying the flow count



CHAPTER 15

Caveats in Cisco IOS XE Release 3.18.6SP

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

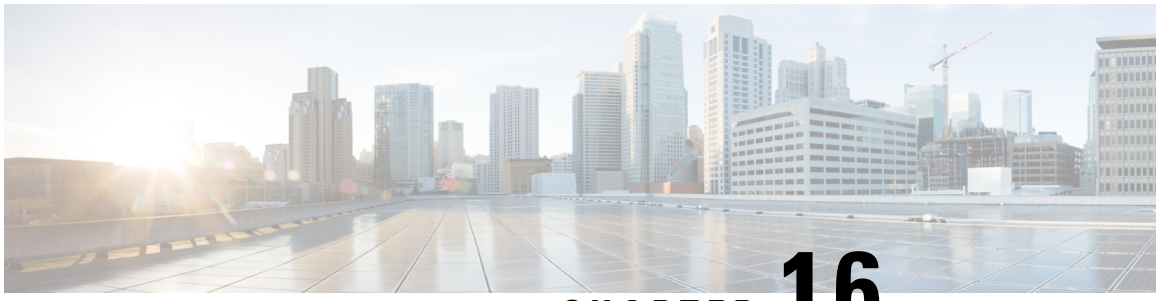
Open Caveats – Cisco IOS XE Release 3.18.6SP

Caveat ID Number	Description
CSCvj75078	RSP3: IOMD crash @ iomd_bsess_open_callback_retry on new active after RP SSO
CSCvk32423	IMA8Z 6-port mode, hwidx not created leading to complete traffic drop
CSCvm04696	Mac learnt on G8032 blocked ports due to DHCPv4 discovery pkts

Resolved Caveats – Cisco IOS XE Release 3.18.6SP

Caveat ID Number	Description
CSCux22473	IPv6 Tracking for route learned from IBGP neighbor is Down.
CSCux68796	IOS-XE Router - High CPU When Handling get-next on "entStateStandby" MIB
CSCuz74957	Cisco IOS and IOS XE Software ISDN Interface Denial of Service Vulnerability
CSCuz99865	IPSec MIB queries returns wrong tunnel count
CSCva00765	Crash after no IPv4 multicast multitopology command
CSCva64842	Observing kernel: EXT2-fs error while moving between polaris and MCP_DEV
CSCve56559	Incorrect Track Resolution Metric for GRE Tunnel
CSCve57830	SUBALTNAME DECODE fails for APIC_EM self-signed cert when validating server identity
CSCve89361	Crash in SISF while processing IPv6 packet
CSCvf11776	VRRPv3 with VRRS remains NOT READY after shutdown Port-channel IF.
CSCvf36269	Cisco IOS and IOS XE Software Network Plug-and-Play Certificate Validation Vulnerability
CSCvf73552	VRRP non-zero authentication data on 16.3.3
CSCvf96294	MIB counter for IPSec tunnels does not decrement under high tunnel scale and churn
CSCvg06142	"ipsm Tunnel Entry" and "Crypto IKMP" memory leak due to IKE tunnel entry not deleted
CSCvg37952	Cisco IOS XE Software ISR4400 Series IPsec Denial of Service Vulnerability
CSCvh54672	VRRP doesnt work over Port-channel L3 interface
CSCvh72848	"no track resolution ip route" and "default track resolution ip route" not working
CSCvh83319	Interop VRRP does not work between C-edge and V-edge
CSCvi83306	Crash with IOSXE-WATCHDOG: Process = IPv6 RIB Event Handler
CSCvj02910	Reload removing IPv6 VRRP group
CSCvj61307	Cisco IOS XE Software Command Injection Vulnerability
CSCvj73544	ospf routing loop for external route with multiple VLINKs/ABRs
CSCvj86790	RIP does not send updates on unnumbered interfaces after reload of ISR 4k
CSCvj98575	Cisco IOS and IOS XE HSRPv2 Information Leak Vulnerability

Caveat ID Number	Description
CSCvk03910	OSPF neighbor stuck in loading after VSS switchover
CSCvk56331	Initial contact in IKEv1 phase 2 rekey (QM1) causes all crypto sessions to drop
CSCvk71047	Router fails to reserve necessary ports for VPN traffic (UDP 500 & 4500) for ISAKMP
CSCvm00765	BFD crash on imitating traffic loss
CSCvm02572	Router crashes on SSH connection with "login on-failure log" enabled
CSCvm28421	ESMC padding is having non-zero random values which is causing duplicate QL-TLV
CSCvm40496	iBGP PE-CE When Route-Reflect enable VRF import all Route Target.
CSCvm51112	"clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys
CSCvm55465	BGP updates missing ISIS advertising-bits led to LDP label purge on peer.
CSCvm62554	BGP multipath feature drops a path from list after BGP update event
CSCvm76070	Not able to enable the CLI http-status-code-ignore
CSCvm92116	Bulk-sync failure due to bgp router-id interface Loopback0
CSCvm93603	IP change on dialer-int does not trigger a correct "local cryto entpt"in DMVPN
CSCvm95236	BGP update not properly processed by inbound route-map
CSCvn07060	Redistributed metric is not be applied if it is in narrow-style
CSCvn28017	ISR4331 Routers May Crash When "eigrp default-route-tag" Configured on IPv4 AF
CSCvn59020	Modified EIGRP timers on Virtual-Template put all associated Vi interfaces into passive mode
CSCvm10079	Force QL Tx option is not working when netsync configured with more than 3 input sources.
CSCvn08456	RSP3: Giant counters incremented for packets bigger than 1500 bytes
CSCvn17722	SONET ACR Pending Object with CEM GROUP interfaces.



CHAPTER 16

Caveats in Cisco IOS XE Release 3.18.5SP

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 Release 3.18.5SP

Caveat ID Number	Description
CSCvb82613	Tunnel or IGP down on SSO due to ingress VOQ packet drop
CSCvd00780	8275.1: PTP Packets are being dropped without untagged EFP on a tagged EFP interface
CSCvd89421	RMEP failure due to CFM HW table corruption

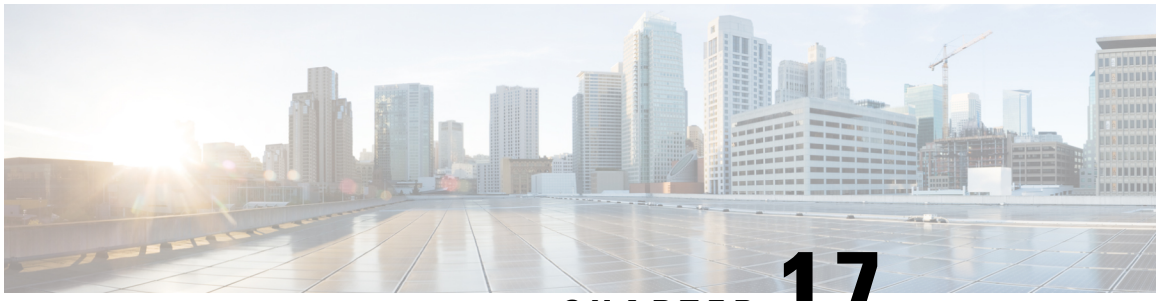
Caveat ID Number	Description
CSCve86912	Giant , Runt, or Pause Frame counters issue.
CSCvf34496	RSP3-QIP: Error objects on Stby cfm_mp_ifh 16794673 sid 3001 download to CPP failed seen upon IM-OIR
CSCvh51179	RSP3: Stale MAC entries are present on a specific scenario which results in ADJ download failure
CSCvk24933	RSP3: QSGMI out of lock with IM OIR and SSO soak
CSCvm04696	MAC learnt on G8032 blocked ports due to DHCPv4 discovery packets
CSCve68911	Nested enhanced route refresh requests triggers stale prefixes.
CSCvf11776	VRRPv3 with VRRS remains NOT READY after shutdown port-channel IF.
CSCvi61745	Crash when running MPLS tunnel protection command
CSCvj02910	Reload removing IPv6 VRRP group
CSCvj43156	Crash in XDR process: fib_rp_table_broker_encode_buf.size <= FIB_RP_TABLE_BROKER_ENC_BUF_SZ
CSCvk22449	BGP Traceback or crash seen with 20k IPv4 BGP scale after reload or clearing bgp
CSCvm00765	BFD crash on imitating traffic loss

Resolved Caveats – Cisco IOS XE Release 3.18.5SP

Caveat ID Number	Description
CSCvk04547	Port-channel member link flap on RP OIR
CSCsd58148	The "%SEC_LOGIN-4-LOGIN_FAILED" does not show username in [user:]
CSCue25168	TPM reserves UDP/4500 for no apparent reason
CSCuy27746	CDP packet causes switch to crash due unexpected exception to CPU vector
CSCuy96461	IOS-XE EPC does not work on port-channel subinterfaces
CSCuz92785	Evaluation of all for NTP
CSCva08142	IOSd crash on LISP enable router
CSCvb71086	CWS with NVI NAT is not working for web traffic
CSCvc07577	Crash in BGP due to regular expressions
CSCvc23569	Evaluation of all for NTP November 2016

Caveat ID Number	Description
CSCvc60745	The tcp_getbuffer memory leak - refcount not reduced when packet dropped
CSCvc98571	EEM applet will not release the Configuration Session Lock if it ends when CLI is in configuration mode
CSCvd21340	IOSd crashed while issuing the **show isdn status** command
CSCvd35443	Site-prefix-learning: crash on EIGRP process when issuing "no ip vrf red" on HMCBR
CSCvd80715	IOSD crash due to memory corruption in aaa accounting
CSCvd80837	Crash observed in DHCP SIP
CSCve00087	Line-by-Line sync verifying failure on command: client test01 server-key 0 Password
CSCve55089	BGP crashes at bgp_ha_sso_enable_ssomode
CSCve76947	EIGRP hmac-sha-256 secret string changes when show running-config is executed
CSCvf21005	config mismatch after code upgraded
CSCvf35507	Crash in SSH Process due to SCP memory corruption
CSCvf63979	Crash when trying to establish new SSH connection
CSCvf67481	AAA process not sending malloc if dynamic heap free mem is under aaa mem threshold
CSCvg02533	router crashed after triggers with debug
CSCvg03444	Hub MC continues to send EIGRP SAF hellos after adjacency removed
CSCvg39082	Cisco device unexpectedly reloads after TCP session timeout
CSCvg48470	ISIS l1-l2 redistribution prefix doesnt get redistributed till clear isis rib redistribution is done
CSCvg67028	VRF deletion status <being deleted> after removing the RD
CSCvg71566	"no cdp enable" is rewritten to "no cdp tlv app" after reload.
CSCvg85879	BGP sets the wrong Local Preference for routes validated by RPKI server
CSCvg87048	Few Stale session are observed during vpdn longetivity
CSCvh06249	Crash when receiving EVPN NLRI with incorrect NLRI length field value
CSCvh55744	SSH password length restricted to 25 for avoiding one of the low impact vulnerability.
CSCvh58909	OSPFv3 cost calculation not correct in some specific topology
CSCvh69518	%SYS-3-TIMERNEG:Cannot start timer with negative offset Process= "ARP Background"

Caveat ID Number	Description
CSCvh96821	ASR1004 started relaying clients' DHCP Discover messages to DHCP Server with the wrong IP address
CSCvi01558	iBGP dynamic peer using TTL 1
CSCvi42002	CDP packets not getting encapsulated over multipoint GRE tunnel
CSCvi52608	CLI show aaa clients detailed command triggered SSH to crash
CSCvi65958	Standby RP crashes due to Memory usage in ospf_insert_multicast_workQ
CSCvi70145	ASR1k | Segmentation fault in dhcp_sip process
CSCvi72479	ISR4K CWS - admission commands override (method-list vs bypass list)
CSCvi74088	link local multicast packets are received when the SVI is in down state
CSCvi93528	PI IOSd reload due to call-home at kex_dh_hash conn pointing to eem
CSCvj29126	RADIUS client on network fails to solicit PAC key from CTS even though the device has a valid PAC
CSCvk10633	bgp crash while running show command and same time bgp peer reset
CSCvk49905	ASR907 RSP3C : Crash when shifting the layer 2 LACP member peer from one link to another



CHAPTER 17

Caveats in Cisco IOS XE Release 3.18.4SP

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 Release 3.18.4SP

Caveat ID Number	Description
CSCva43417	E1 Interfaces go DOWN on remote alarm (RDI)
CSCvb01698	LEAPSEC: leap second is not considered while setting PTP to system time
CSCvb96943	Offset from master jumps to Huge value with SPAN

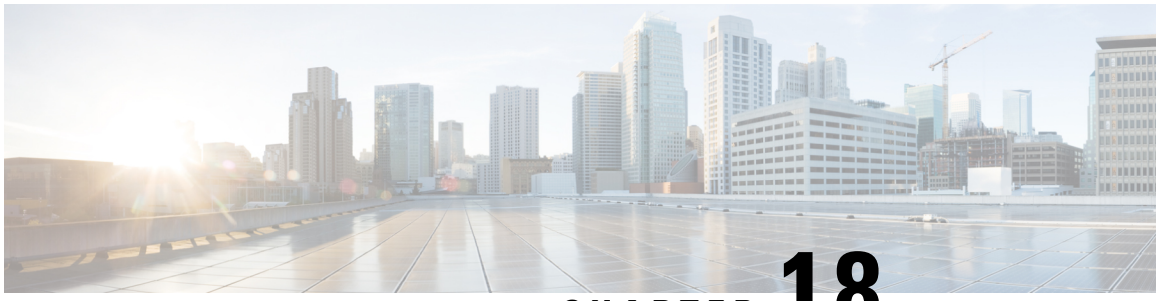
Caveat ID Number	Description
CSCvc59436	RSP3:Delay in updating egress efp stats for Tengig interfaces
CSCvd44667	RSP3: PREFIX Object Errored Objects on Local Core Flaps and in Parallel on Other Routers in the Core
CSCvd50734	RSP3-200:Router Crash while trying to delete label uea_oce_base_delete uea_mpls_label_delete_async
CSCvd77735	RSP3 - Small loss (6-10ms) observed for VPLS traffic when BGP backup peer is powered down
CSCvd89421	RMEP failure due to CFM HW table corruption
CSCve05859	Exxx EIN: G.8275.1 testing: Clock loop forming between synce and ptp
CSCve14324	RSP3C : port level shaper is counting packets twice.
CSCve43404	PTP Clock Creation Fails for Specific Sequence of Triggers
CSCve78337	MLP MRAPS Convergence is high on Work-Active SSO node
CSCve86912	[Counter]: Giant/Runt/Pause Frame counters issue.
CSCvf08577	RSP3 Arad not able to timestamp higher stream id packets in default profile
CSCvf08656	RSP3 : Traffic failure for few Labelled BGP prefixes (BGP label imposed is incorrect)
CSCvf09940	RSP3_2x10GE: output netsync drifting after SSO when locked to 2x10GE
CSCvf16468	RSP3-QIP: CFM H/w offloaded sessions over xconnect affecting S/w sessions configured over BD
CSCvf19136	Debugability : show platform software agent iomd <> np datapath hdlc <CEMA-ID>
CSCvf21748	RSP3-QIP: Traffic flowing though TEFP is shut in G8032 ring
CSCvf34496	RSP3-QIP:Error objects on Stby cfm_mp_ifh 16794673 sid 3001 download to CPP failed seen upon IM-OIR
CSCvf45267	RSP3 - Loadbalance map not getting deleted (IM OIR)
CSCvg84699	BFD session not coming up on RSP3 due to wrong platform offload limit
CSCvg99675	RSP3:Transient FRR download failure during soak testing
CSCvh15762	RSP3: IOSd Crash in FastPath Thread during Punt Packet Buffer Dequeue on ARP Flaps Soak
CSCvh51179	RSP3: Stale Mac entries are present on a specific scenario which results in ADJ download failure
CSCvh77868	ASR-903 (RSP3_400) fsck of bootflash returned error code 8. Recommend reformatting
CSCvi02398	snmp mib and device configs not matching

Caveat ID Number	Description
CSCvi06300	RSP3: Pending issues seen when converting from Access EFP's to Trunk EFP's
CSCvi06358	Label and outgoing interface programmed wrongly for prefix in RSP3

Resolved Caveats – Cisco IOS XE Release 3.18.4SP

Caveat ID Number	Description
CSCui67191	Cisco IOS XE Software Ethernet Virtual Private Network Border Gateway Protocol DOS Vulnerability
CSCuy30341	Failed to create, Pseudowire interface
CSCvb96911	OSPF NSSA Translator ABR does not Translate Type 7 to 5 with only VRF Superbackbone as non-NSSA area
CSCvc38538	IPSLA Y1731 start time is much greater than sysUpTime while doing snmpwalk
CSCvc61899	static route is not getting redistributed into RIP database
CSCvc63685	%QOS-4-INVALIDBW: errors occur on reboot when policing is used
CSCvd38391	Standby Router: uea_mgr crashed @ ml2vpn_provision_pw_and_ac
CSCve37398	RSP3-L2VPN: Load balancing is happening based on wrong fields in P node when CW is enabled.
CSCve64336	RSP1-Continous ESMC tracebacks observed after IMA8T OIR followed by SSO
CSCve64341	Mid Point LSP creation failure after reload with latest polaris Image
CSCvf30801	RSP3-QIP: LTM b/w CEs not working if MIP is configured on PE participating in VPLS
CSCvf51341	Crash after show ip ospf database summary command
CSCvf52432	RSP3:Pending-issues & Ack upon defaulting all core interfaces in VPLS scale setup
CSCvf55306	Static route of which next-hop intf is GRE tunnel remains even if the tunnel is down
CSCvf56274	BGP VRF route redistribution into global routing table fails after a VRF route flap
CSCvf62916	Router crashes when doing "show ip bgp neighbor" on a flapping BGP neighborship
CSCvf63541	BGP w/global import/export crashes when several nbrs deleted simultaneously
CSCvf67269	IS-IS support for mult-instance redistribution for IPv6.
CSCvf72154	RSP3 - PIM neighborship down on BDI interface due to packets ASIC loop.
CSCvf76512	Option 82 circuit-id-tag restricted by 6 bytes

Caveat ID Number	Description
CSCvf80495	IPv6 BGP network advertized not seen in the peer
CSCvf82663	RSP3C crashed at dl_callback
CSCvf84349	Router crash on polling cEigrpPeerEntry
CSCvf95077	Stale Mac entry in MLRIB
CSCvg03308	[RSP3-DHCP-Relay]:unicast dhcp relay is getting dropped in transparent case with HSRP/VRRP/GLBP
CSCvg03542	[RIB route watch] detect stale pointer from client to avoid system crash with corrupted memory
CSCvg07169	D6 Update attribute Total Bandwidth = 37901kbps is incorrect
CSCvg28721	RSP3:uea-mgr crashed while trying to install a label entry in kbp(update case)
CSCvg42691	RSP3- P node ECMP loadbalancing failing for ip traffic
CSCvg43975	RSP3: Leak in G8032 IOS TDL Messaging on Flapping the Ring
CSCvg48485	RSP3 - Ingress LDP label incorrectly programmed to FEC 0x0
CSCvg70173	Not able to configure xconnect untagged service instance with EVPN under the same interface
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 ASR903 RSP3C after link flap
CSCvh20968	Multicast traffic not forwarded on VPLS after trigger
CSCvh51377	RSP3_400 : False Tx bias violation alerts seen on console with CPAK-100G-LR4 SFP's
CSCvh71856	IOSd crash when enabling dot1q in a port-channel sub-interface



CHAPTER 18

Caveats in Cisco IOS XE Release 3.18.3SP

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

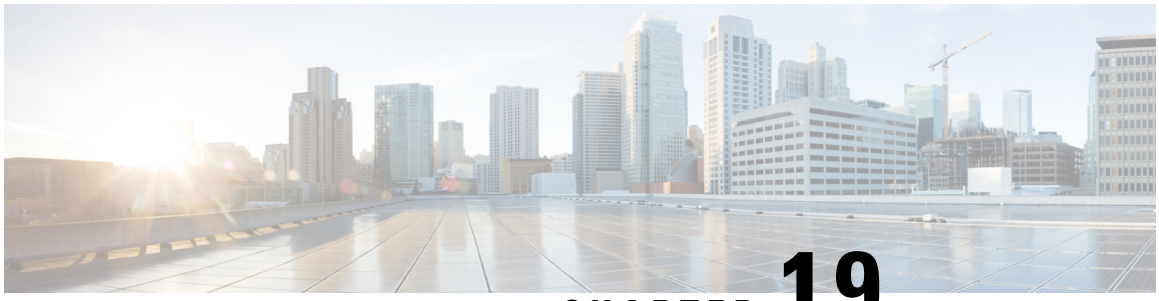
Open Caveats – Cisco IOS XE Release 3.18.3SP

Caveat ID Number	Description
CSCvd89421	RMEP failure due to CFM HW table corruption
CSCvf30801	RSP3-QIP: LTM b/w CEs not working if MIP is configured on PE participating in VPLS

Caveat ID Number	Description
CSCvf34496	RSP3-QIP:Error objects on Stby cfm_mp_ifh 16794673 sid 3001 download to CPP failed seen upon IM-OIR
CSCvd77735	Small loss (6-10ms) observed for VPLS traffic when BGP backup peer is powered down
CSCve87759	Link flaps on configuring G8275.1

Resolved Caveats – Cisco IOS XE Release 3.18.3SP

Caveat ID Number	Description
CSCvd69942	100% ipv6 packet drop for downstream traffic on ASR903 (RSP3C) when RPL state changes.
CSCvf21127	2 AC's in a VFI, when one interface is shutdown, traffic is not flood to other interface
CSCve10269	RSP3 unable to route(drops) unicast dhcp packets with giaddr field as 0.0.0.0
CSCve77231	RSP3:traffic failure on VRRP session and traces @ vrrp_comms_process_pak
CSCve10547	[RSP3-DHCP]:rsp3 is dropping dhcp bootp packets with sorc port 4011 and dest port 67/68
CSCvd34788	ASR903 with RSP3 might crash with reason bulk sync failure
CSCvf40636	RSP3-200:Observing Packets drops if the Line Rate is more than 32%
CSCvd00780	8275.1: PTP Packets are being dropped without untagged EFP on a tagged EFP interface



CHAPTER 19

Caveats in Cisco IOS XE Release 3.18.1SP

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 Release 3.18.1SP

Caveat ID Number	Description
CSCuz39371	STS-1 path behavior problem upon controller shut.
CSCuz51456	TSOP OC3, POS takes 1-10 seconds for convergence on SSO.
CSCuz97551	OC-X duplicate alarm messages and filtering of alarms.

Caveat ID Number	Description
CSCva16169	DS1: Traffic is not resuming after Ctrl shut then SSO and no shut.
CSCva54675	Incorrect Input/Output rate counters on T1/T3 CEM interface.
CSCva77248	OCx APS-ACR ACR-DCR: ACR/DCR is not enabled for CT3 mode for T1 5.
CSCvb05110	ACR not able to remove CEM configurations if no single physical controller is configured.
CSCvb17783	RSP3C leak of PMF protection pointer resource.
CSCvb24067	PMON cleanup.
CSCvb35480	Port-channel flaps when OIR of RSP is done on RSP1.
CSCvb51372	CEM jitterbuffer underruns with CEM marking policy.
CSCvb57740	OCN IM crash post IM FPGA upgrade + SSO.
CSCvb59196	RSP3 : Ping/traffic failure on IPSec tunnels after SSO.
CSCvb61221	RSP3 : IKEv2 IPSec tunnels stay down after ISSU.
CSCvb63314	Traffic not egressing out on AC after standby PW became active PW.
CSCvb67543	uea mgr crash@uea_mpls_atom upon flapping core A/A Port-channel interface of peer box.
CSCvb68652	VTCEP AIS and B3 alarms on SSO and few DS1/VT1.5 SATOP with AIS.
CSCvb71584	Bulk-sync failure - T3 clock source internal.
CSCvb73784	dhcp_snooping_platform_parse_evc_cid: idb not found for IMs on bay 15.
CSCvb75091	RSP3C is sending tagged PTP packets to downstream node.
CSCvb77215	RSP3 : 6PE/6VPE traffic drop on SSO for approximately 30-40sec with VRRP.
CSCvb77938	DS3: On channelized T1, AIS is not reporting properly.
CSCvb78285	OCx: Iomd crash on active RSP post SSO of admin down IM.
CSCvb78369	OCX: Standby RSP crashed with hw-module stop.
CSCvb84096	“no channelized” configurations are not saved for the DS3 ports.
CSCvb84308	CLIs are not accepted for path configured as T3 mode.
CSCvc03169	l2protocol tunnel issue with Port-channel numbers >32.
CSCvc03451	RSP3: Management interface is not accepting manual speed (10/100 Mbps).

Open Caveats – Cisco IOS XE Release 3.18.1cSP

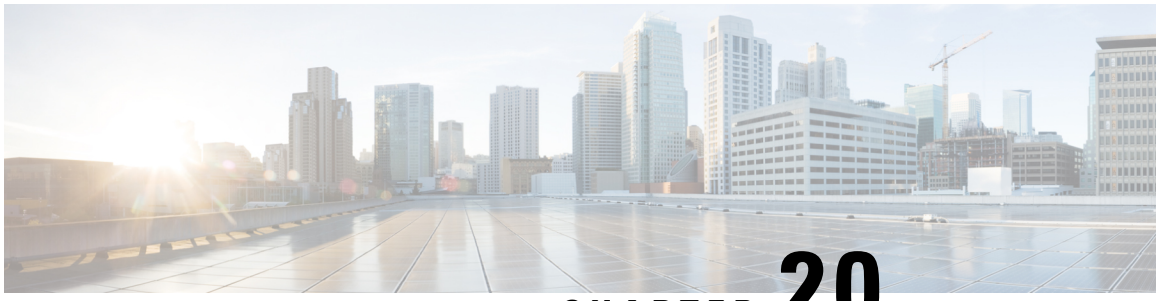
All open caveats that apply to Cisco IOS XE Release 3.18.1SP also apply to Cisco IOS XE Release 3.18.1cSP.

Resolved Caveats – Cisco IOS XE Release 3.18.1SP

Caveat ID Number	Description
CSCuy07786	RSP3: ECMP load-balance for TAG-TO-TAG in hardware does not work.
CSCuy11711	TIM-S, TIM-P, and TIM-V fields are not showing on show controller output.
CSCuy46447	Flex-LSP: Tunnel flap is observed when W-LSP BFD goes down after reopt.
CSCuz90585	RSP3: Egress filtering rule might fail here messages on configuring T-EFP.
CSCva06999	ACR/DCR clock state is not changing for shut on CE after SSO.
CSCva13798	RSP3: Uea mgr crashs on "show mac-address-table secure" command.
CSCva14621	ptpd_uea crash due to watchdog due to mutex deadlock
CSCva21655	BDI MPLS MTU cannot be set more than 1500.
CSCva27910	DS3 Jitterbuffer underruns/overruns.
CSCva38115	SMMac on EFP not getting flushed out on deleting and reconfiguring the BD.
CSCva39555	MPLS forwarding issue.
CSCva52316	uea_mgr crash is observed after multiple shut/no shut xconnect.
CSCva71102	"cefcFanTrayOperStatus" to provide a state "warning(4)" for fan failures.
CSCvb18966	mlacp standby POA link forwards multicast/broadcast traffic after reboot.
CSCvb49938	UDP packets are getting corrupted in MPLS De-Agg case.
CSCvb61160	RSP3: HW-LB: L3VPN - Path is preselected though PIC is enabled.
CSCvb83576	Crash and reboot when set OSPFv3 auth and IPv6 BDI and Port-channel.

Resolved Caveats – Cisco IOS XE Release 3.18.1cSP

All resolved caveats that apply to Cisco IOS XE Release 3.18.1SP also apply to Cisco IOS XE Release 3.18.1cSP.



CHAPTER 20

Caveats in Cisco IOS XE Release 3.18SP

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 Release 3.18SP

Caveat ID Number	Description
CSCva07472	Inconsistency with Vcop SFP compatibility on NCS4202
CSCva16169	DS1:Traffic not resuming after Ctrl shut then SSO and No shut
CSCuz26189	Standby crashed after several iterations of Config/Unconfig script
CSCva14263	DS3 IM: IOMD crash on slot 10 in DSx loaded setup over router reload

Caveat ID Number	Description
CSCva27910	DS3 Jitterbuffer underruns/overruns
CSCux74888	DS3: uea_mngr crash seen after multiple IM hard OIR
CSCuz49527	slot 5 in 907/4216,intermittent drop & traffic down post router reload
CSCuz95664	OC3 IM Runs Out of FIFO Buffer on Reassembling MLPPP Fragments
CSCux45450	OC3 IOMD CPUHOG on SOAK Test of SONET Shut and No Shut
CSCuz95621	OC3 IOMD Crash on RP SSO while MLPPP Scale Sessions Flap
CSCuz51456	TSOP OC3 , POS takes 1-10 seconds to Convergence on SSO
CSCva06999	ACR/DCR Clock state is not changing for shut on CE after SSO
CSCva14445	OCN IM FPGA Upgrade fails with ISSU
CSCuz78113	OCx HA: Traffic outage is seen during SSO for few ckts at 4K scale
CSCva05301	4xOC3 IM unable to reset itself after IM FPGA upgrade
CSCva41678	OC3 IM continuously rebooting after shutdown at high temperature