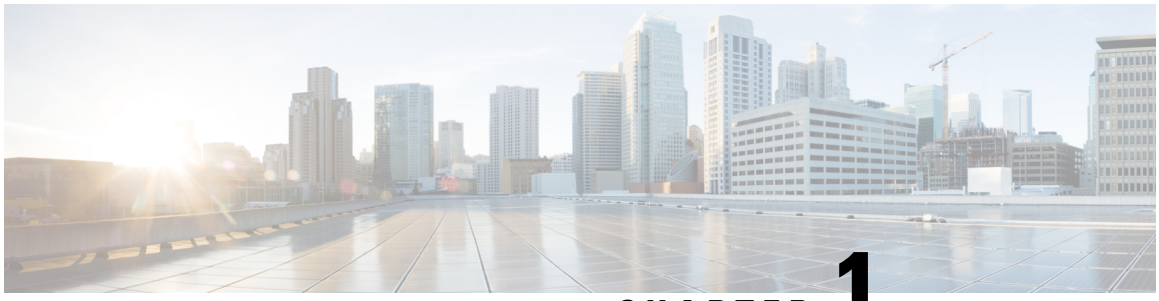
Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE 3.18SP

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

CONTENTS



CHAPTER 1

Introduction

This document provides information about the IOS XE software release for the Cisco NCS 4201 and Cisco NCS 4202 beginning with Cisco IOS XE Everest 16.5.1, which is the first supported release in the Release 16 Series.

Cisco NCS 4201 and Cisco NCS 4202 Overview

The Cisco NCS 4201 and NCS 4202 Network Convergence Systems are full-featured, compact one-RU high converged access platforms designed for the cost-effective delivery of TDM to IP or MPLS migration services. These temperature-hardened, high-throughput, small-form-factor, low-power-consumption systems are optimized for circuit emulation (CEM) and business applications. NCS 4201 and NCS 4202 chassis allow service providers to deliver dense scale in a compact form factor and unmatched CEM and Carrier Ethernet (CE) capabilities. They also provide a comprehensive and scalable feature set, supporting both Layer 2 VPN (L2VPN) and Layer 3 VPN (L3VPN) services in a compact package .

For more information on the Cisco NCS 4201 Chassis, see the Cisco NCS 4201 Hardware Installation Guide.

For more information on the Cisco NCS 4202 Chassis, see the Cisco NCS 4202 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 table list the hardware supported for Cisco NCS 4202 chassis.

Chassis	Supported Interface Modules	Part Numbers
NCS 4202	8 port T1/E1 CEM Interface Module	NCS4200-8E1T1-CE

Determining the Software Version

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

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

ROMMON Version

- NCS4201—15.6(31r)S
- NCS4202—15.6(24r)S

Bundled FPGA Versions

The following are HoFPGA versions bundled in the IOS:

- NCS4201—0X00030015
- NCS4202
  - BFD—0X0003001c
  - Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—0x10050071

The following are HoFPGA versions bundled in IOS for 16.12.7 and 16.12.6 releases:

- NCS 4201— 0X00040019
- NCS 4202—
  - BFD—0X0003001b
  - Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—NA

Limitations and Restrictions on the Cisco NCS 4201 and Cisco NCS 4202 Series

- The default interface command is used to default the parameters under that interface. However, when speed is configured on the interface, the following error is displayed:

  ```
  Speed is configured. Remove speed configuration before enabling auto-negotiation
  ```

- SSFPs are not supported.
- Virtual services should be deactivated and uninstalled before performing replace operations.
- For Cisco NCS 4202 Series:
  - Interface naming is from right to left. For more information, see the Cisco NCS 4200 Series Software Configuration Guide .
  - Packet size greater than 1460 is not supported over IPsec Tunnel.
  - Minimal traffic drop might be seen for a moment when higher rate traffic is sent through the IPsec tunnels for the first time.
  - IPsec is only supported for TCP and UDP and is not supported for SCTP.

Known Issues

Identifier	Description
CSCux22026	supress syslog messages while booting up for internal interfaces

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.

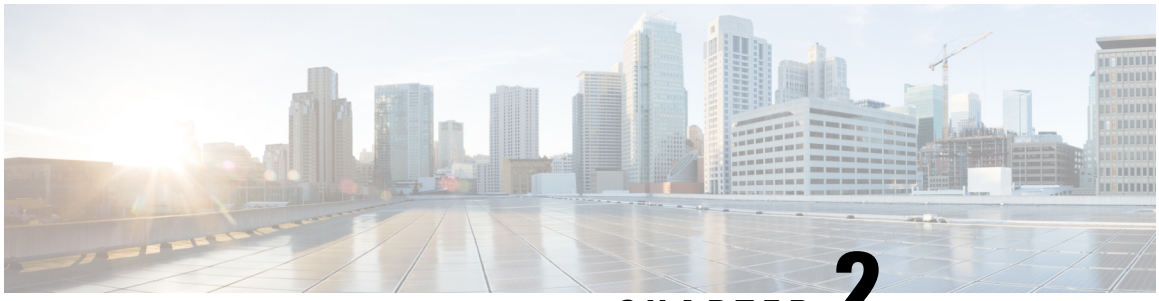
MIB Support

To view supported MIB, go to http://tools.cisco.com/ITDIT/MIBS/MainServlet.

Accessibility Features in the Cisco NCS 4201 and Cisco NCS 4202 Series

For a list of accessibility features in Cisco NCS 4201 and Cisco NCS 4202 Series, see the Voluntary Product Accessibility Template (VPAT) on the Cisco website, or contact accessibility@cisco.com.

All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.



CHAPTER 2

New Features in Cisco IOS XE Release 3.18.9SP

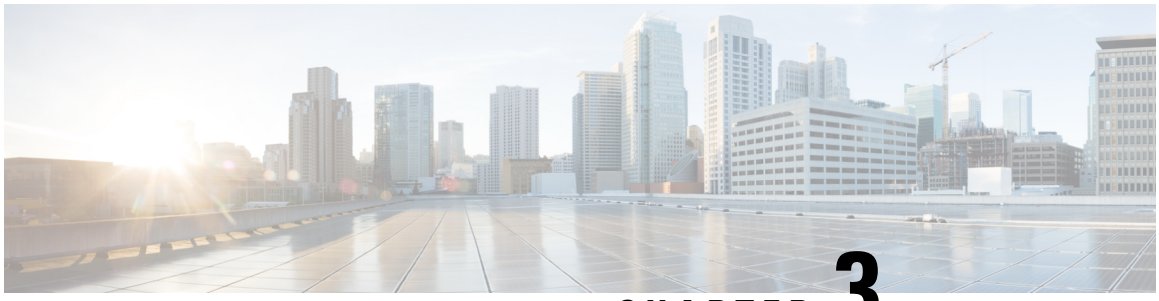
This chapter describes the new features supported on the Cisco NCS 4200 Series.

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

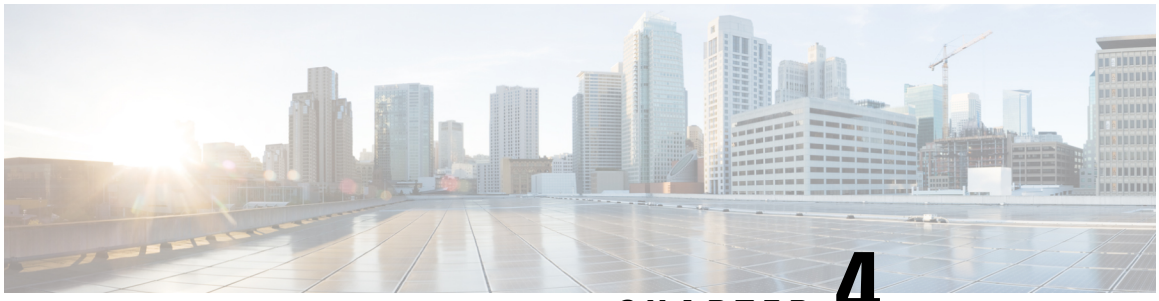
This chapter describes the new features supported on the Cisco NCS 4200 Series.

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

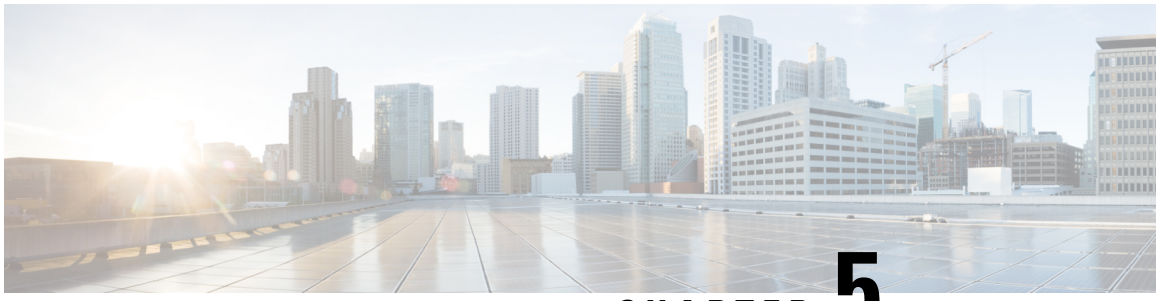
This chapter describes the new features supported on the Cisco NCS 4200 Series.

New 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

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



CHAPTER 5

New Features in Cisco IOS XE Release 3.18.6SP

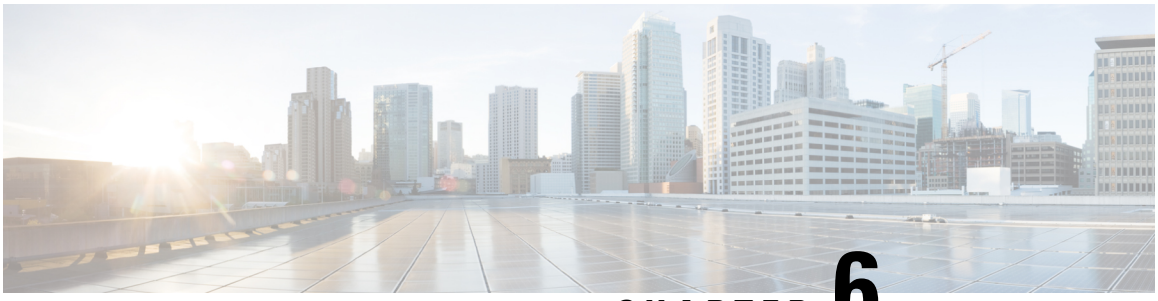
This chapter describes the new features supported on the Cisco NCS 4200 Series.

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 6

New Features in Cisco IOS XE Release 3.18.5SP

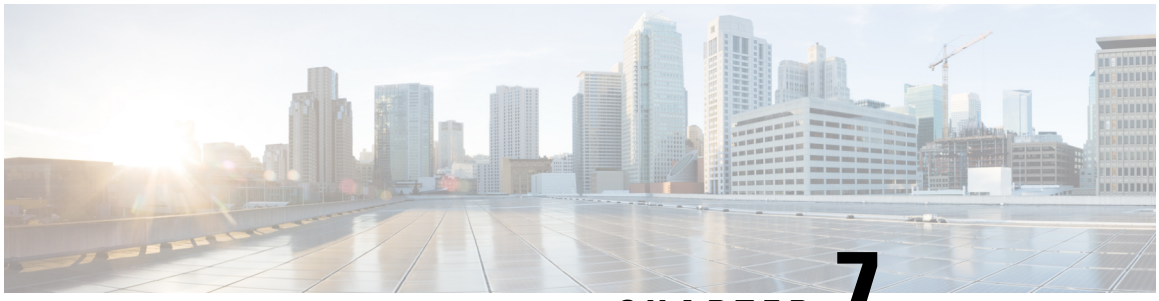
This chapter describes the new features supported on the Cisco NCS 4200 Series.

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 7

New Features in Cisco IOS XE Release 3.18.4SP

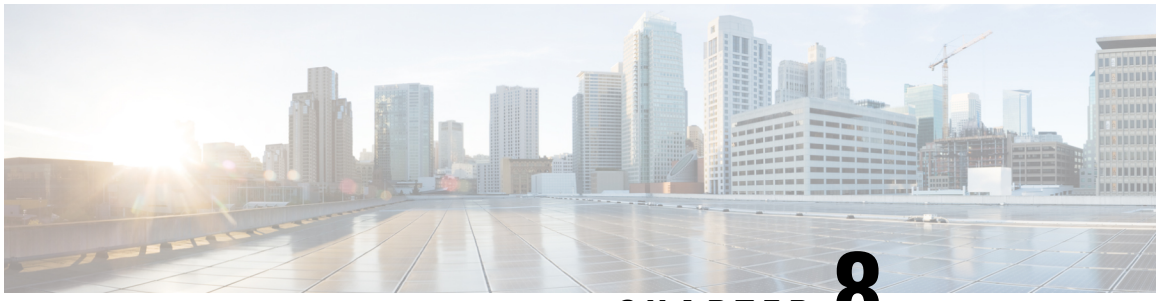
This chapter describes the new features supported on the Cisco NCS 4200 Series.

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

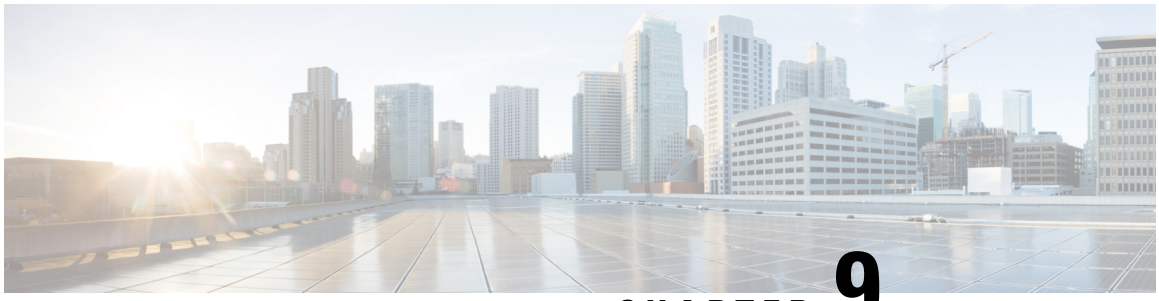
This chapter describes the new features supported on the Cisco NCS 4200 Series.

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

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



CHAPTER 9

New Features in Cisco IOS XE Release 3.18.3SP

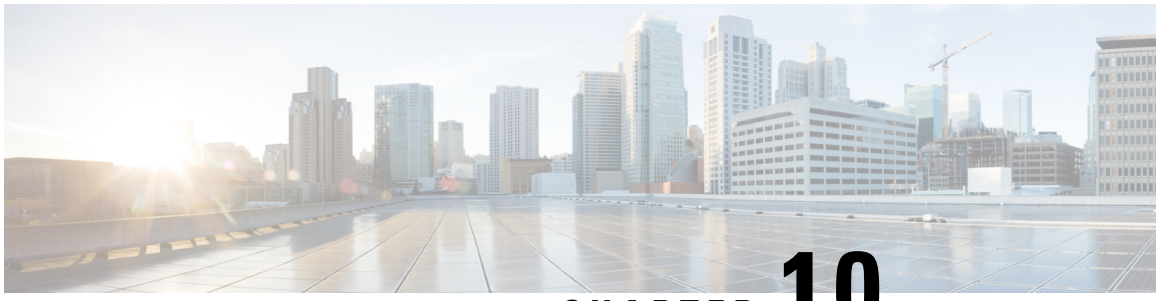
This chapter describes the new features supported on the Cisco NCS 4200 Series.

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

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

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:

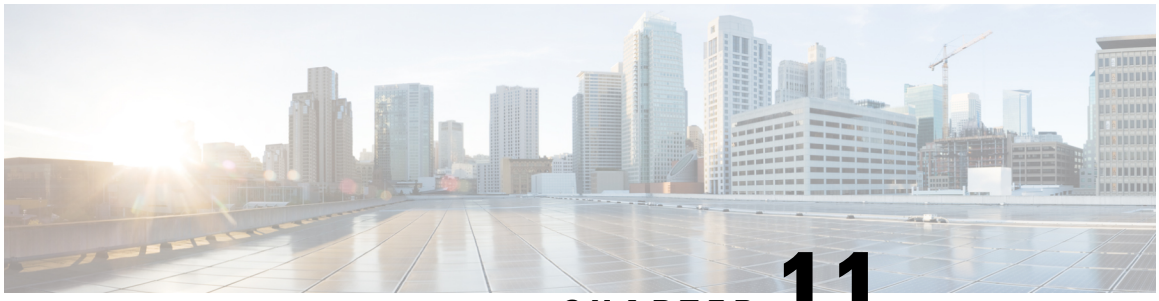
  - leap-second
  - offset

  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.



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 for Cisco IOS XE Release 3.18SP

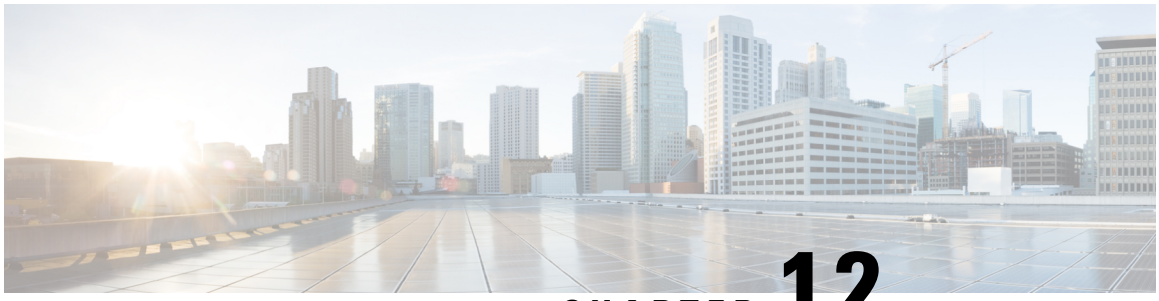
The following chassis were introduced:

- Cisco NCS 4201 Series—The Cisco NCS 4201 is a modular and fixed configuration chassis that enables service providers to provide business, residential, and mobile access services to their users. It is the Carrier Ethernet access platform providing Ethernet services.

  The Cisco NCS 4201 Series complements and extends Cisco's current and planned Carrier Ethernet routing portfolio providing a cost optimized, and extended temperature range access platform.

- Cisco NCS 4202 Series—The Cisco NCS 4202 Series is a family of fixed configuration chassis that provides common network architecture to the Service Providers for macro and small cell networks.

  This chassis acts as an access device for mobile backhaul services-macro Cell Site chassis (CSR) and Small Cell chassis (SCR). As an access device, it provides capabilities like 1GE/10GE, MPLS, H-QoS, Services, GPS clocking, PoE and fit within ETSI 300 mm depth cabinet. It can easily be integrated into the Unified MPLS for Mobile Transport (UMMT) and Fixed Mobile Convergence (FMC) solution.



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.

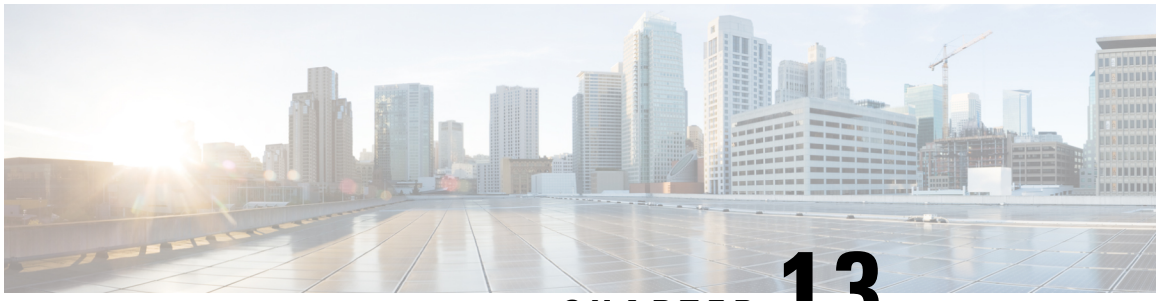
- Open Caveats – Cisco IOS XE Release 3.18.9SP, on page 29
- Resolved Caveats – Cisco IOS XE Release 3.18.9SP, on page 29

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 3.18.8a

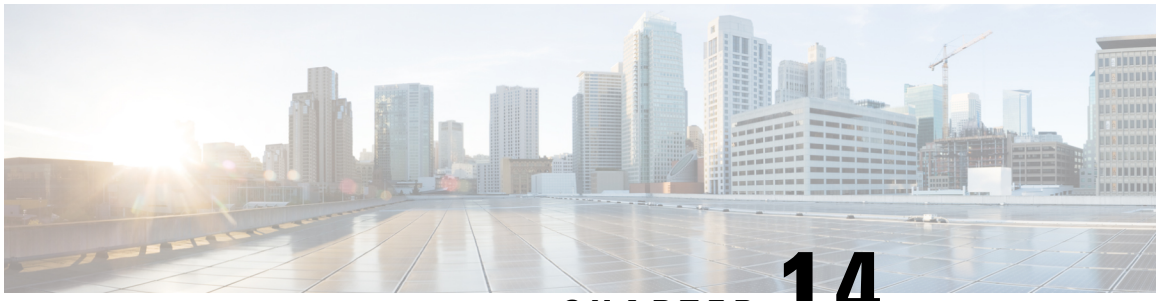
Caveat ID Number	Description
CSCvo07619	ASR920-BDI IPv6 ping failure_FMFP_OBJ_Download_Failure
CSCvp01189	Broadcast storm control triggers without any Broadcast traffic, cont...

Resolved Caveats – Cisco IOS XE Release 3.18.8aSP

There are no resolved caveats in this release.

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
CSCvo07619	ASR920-BDI IPv6 ping failure_FMFP_OBJ_Download_Failure
CSCvp01189	Broadcast storm control triggers without any Broadcast traffic, cont...

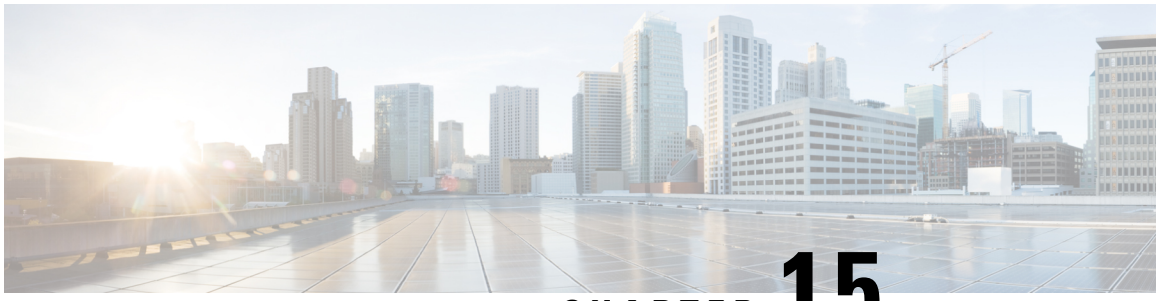
Resolved Caveats – Cisco IOS XE Release 3.18.7SP

Caveat ID Number	Description
CSCvg08224	G8265.1: PTP flaps between HOLDOVER and LOCKED with 64/64 packet rate and HOTSTANDBY
CSCvg21913	AMS port netsync is not up on reload
CSCvm12382	ASR-920-12CZ | Netflow entires not created if SDM template is initialised on affected release.
CSCvq33362	Vendor specific GLC-BX-D optics not working in ASR920

Resolved Caveats – Cisco IOS XE Release 3.18.7SP Platform Independent

Caveat ID Number	Description
CSCvb05793	traffic drop observed upto 2 mins on active Sup pull with ECMP
CSCvf20607	ASR1K RSP crash when command 'show ip rsvp sender detail' was executed
CSCvh62861	IOSd crash @ NHRP nhrp_group_tunnel_qos_remove
CSCvj43156	Crash in XDR process: "fib_rp_table_broker_encode_buf.size <= FIB_RP_TABLE_BROKER_ENC_BUF_SZ"
CSCvk17998	Rekey Timer are same for both the Server and Client
CSCvm64865	[EIGRP] a summary route is updated by an external route
CSCvn00218	CUBE Crash in sipSPIAppAddCallInfoUI
CSCvn56017	Crash while processing ISIS updates when DiffServ-TE is enabled
CSCvn93524	Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability
CSCvo55194	After RSP switchover label imposition was not programmed in Software on APS standby router
CSCvo66216	IPSec-Session count in "show crypto eli" reaches max causing VPN failure
CSCvp76434	OSPF summary-route (Type 5) redistribute into ospf via 'summary-address' cmd is not install in RIB
CSCvp78236	Crash during SNMP Configuration, ospfv3_pdb_from_router_info
CSCvp81102	IPsec SA installation fails with simultaneous negotiations despite fix for CSCve08418

Caveat ID Number	Description
CSCvp87125	Default-route is not installed in Local PE VRF if there is 0.0.0.0/X route present in routing table
CSCvp99881	BGP set wrong local preference for routes in RPKI invalid state
CSCvq19673	Evaluation of asr1k for TCP_SACK
CSCvq46617	RLFA config causing OSPF to ignore backup path addition for NSSA prefix after primary link flap
CSCvq67901	Crash in HTTP core process



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

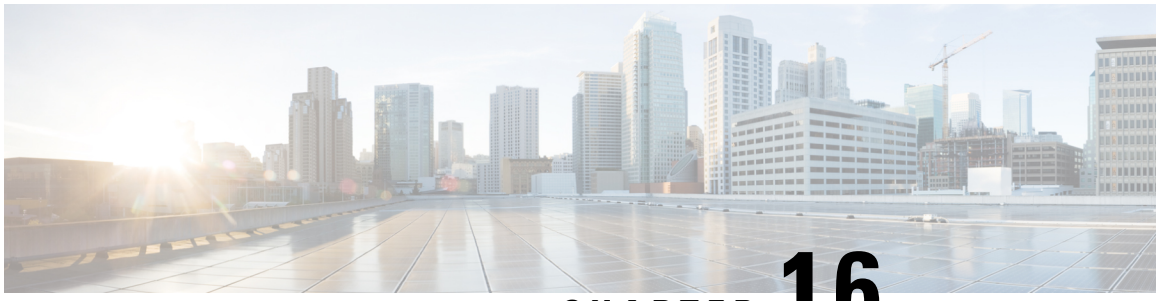
Open Caveats – Cisco IOS XE Release 3.18.6SP

Caveat ID Number	Description
CSCvp01189	Broadcast storm control triggers without any Broadcast traffic, cont...

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
CSCvi96811	[HS]: PTP scale test fails with 64 slaves
CSCvj43977	CEF inconsistency issue observed after continuous BFD flaps.
CSCvk05865	AIS: box crashed at zl303xx_AprRemoveServer
CSCvm13858	Complete Traffic Loss for Existing TEFP Services on New VLAN Add and Remove
CSCvm27110	cefcFRURemoved trap is generated for fixed IM module
CSCvm76155	Input Flows are only seen on the collector- output flows are not exported on ASR 920
CSCvn18271	Link status LED of ASR-920-12SZ-IM MGMT port was keep displayed as green even port is shutdown.
CSCvn47230	Qos imapct service : Incorrect classification observed on Prouter in mpls core.
CSCvn63516	Ports not comming up after 12x1GEupgradelicense installation
CSCvo19770	Router crashes at hashtable_get_nth_entry



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
CSCve08311	CFM ping failing if configured interface is holding SSFP
CSCve36953	ASR920: L2 Bridge-domain Forwarding Fails as Packets Dropped in PreMET
CSCvh90836	Kernel - The Unknown OBFL crash due to swapper task process

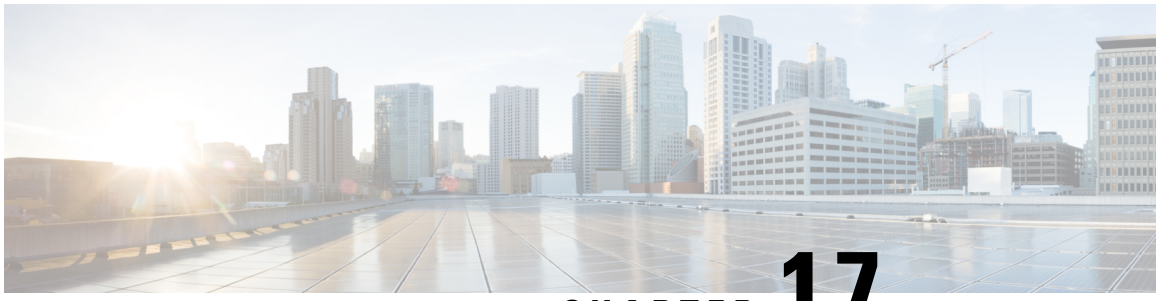
Caveat ID Number	Description
CSCvi56478	Ping failure from ASR920 to ASR903 - EAMapperError1 counter after upgrade to specific ES image
CSCvj69019	RJIL: 10G CRC error in ASR920
CSCvk05865	AIS: box crashed at zl303xx_AprRemoveServer
CSCvk35460	Counter not increasing under show interface
CSCvm21736	The negotiation auto configuration gets removed from dual rate ports post node hard reset or power cycle
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
CSCvg43968	Cylon manager crash with adjmgr_get_fid_index
CSCvg65763	TOD Cisco format got broken.
CSCvg93982	IOS XE entSensorThresholdNotification trap is not generated for card temperature
CSCvi42821	ASR920 crashes when polling CISCO-CDP-MIB in crete_hide_ipsec_port
CSCvj00222	Intermittent packet drops for small size VRF ping (64-72)
CSCvj11708	ASR 920 crash in RP0 cylon mgr when a BDI was created
CSCvj44239	ASR920 reloads with an IOSD crash @ mcp_nv_write
CSCvk12131	Downgrade 16.10: sdm template changes from max-qos-video to unknown in 3.18SP and netflow-video in 16.9
CSCvk58239	ASR920: PSU removal and insertion results in router stuck.
CSCvk65739	A900-IMA2Z will not come online after upgrade to 3.18.3SP

Caveat ID Number	Description
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
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

Caveat ID Number	Description
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"
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

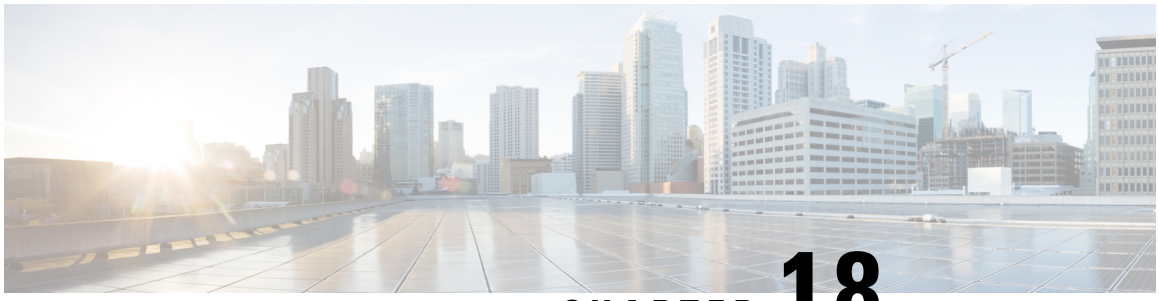
Caveat ID Number	Description
CSCux20143	RSP3/BFD:[new]Timeout not happening after shut of link with host traffic
CSCuz82303	Setting MTU to 9216 on routed interface causes scheduler(BRP/BRR) fail
CSCva43417	E1 Interfaces go DOWN on remote alarm (RDI)

Caveat ID Number	Description
CSCva61618	SADT throws Warnings more than one time for more iterations
CSCvb01698	LEAPSEC: leap second is not considered while setting PTP to system time
CSCvb96943	Offset from master jumps to Huge value with SPAN
CSCvd58258	IOS-XE display issue show hw-module subslot X/X transceiver X idprom detail
CSCve43404	PTP Clock Creation Fails for Specific Sequence of Triggers
CSCve54554	IM will not warn when copying an invalid image
CSCvg88747	IOS hung and stuck in loop if there is any issue in USB port
CSCvi02398	SNMP MIB and device configs are not matching
CSCvi18644	BFD flaps during SSO

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	Skywalker: 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
CSCvd87285	Display issue - Egress i/f and L2 stats shows "unknown" and no packet drops
CSCve64336	RSP1-Continous ESMC tracebacks observed after IMA8T OIR followed by SSO
CSCve64341	Mid Point LSP creation failure after reload with latest polaris Image
CSCvf51341	Crash after show ip ospf database summary command
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

Caveat ID Number	Description
CSCvf67269	IS-IS support for mult-instance redistribution for IPv6.
CSCvf76512	option 82 circuit-id-tag restricted by 6 bytes
CSCvf80495	IPv6 BGP network advertized not seen in the peer
CSCvf83216	Negative broadcast counters on port channel interface after clearing the counters
CSCvf84349	Router crash on polling cEigrpPeerEntry
CSCvf95077	Stale Mac entry in MLRIB
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
CSCvg14825	Require varbind entSensorPrecision,Scale & Type along with trap entSensorThresholdNotification
CSCvg70173	Not able to configure xconnect untagged service instance with EVPN under the same interface
CSCvg85163	ZTP not triggered with Gratuitous ARP
CSCvg97160	IM Tengig interface MTU has not been set more than 1500 in H/W
CSCvh71856	IOSd crash when enabling dot1q in a port-channel sub-interface
CSCvh86486	IM: routers issue with sfp-h10gb-cu1m cabling



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

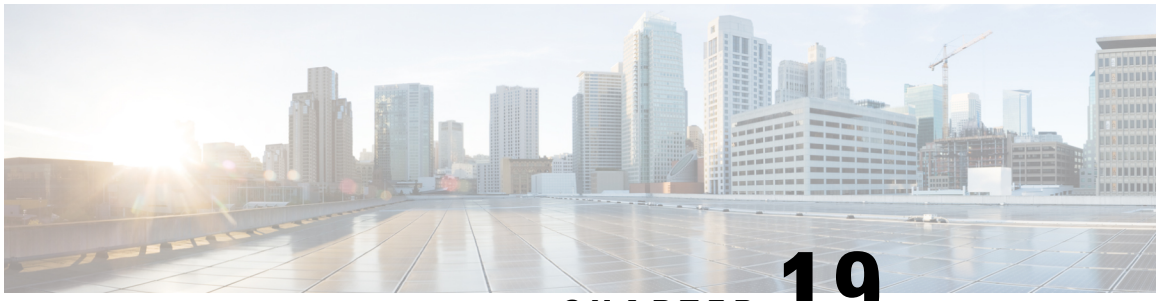
Caveat ID Number	Description
CSCvf46252	Crash in cylon_mgr when MPLS TE interface shut down
CSCvf03668	Mid-chain ADJ Error Object on MPLS TE Tunnel Interfaces and Core Gig Flap SOAK
CSCve54813	PUNT_KEEPALIVE Fail and Cylon_Mgr Crash in Adjacency Manager on Reload Soak of Peer

Caveat ID Number	Description
CSCvf11756	EOMPLS traffic drop over tunnel interface after Tunnel Flap (EL3IDC is not updated properly)
CSCvf35944	XE318SP3-MCAST_hardening: P2MP-Te : Traffic drop with "clear ip mroute *"

Resolved Caveats – Cisco IOS XE Release 3.18.3SP

Caveat ID Number	Description
CSCvd52872	IPv4 ACL is still active when deleted from interface configuration
CSCvc47552	IPv6-access list with fragments dropping non fragments packets
CSCva27296	Enhance the show command to dump the DDR interrupt registers.
CSCvf43516	Storm Control when using BPS - Counters incorrect
CSCvf10067	Broadcast Storm detected when interface is brought up.
CSCvb32221	L2: OSPF over untag BDI failed after switching from tagged BDI to untag.
CSCve37021	MPLS_PACKET-4-NOLFDSB: MPLS packet received on non MPLS enabled interface
CSCve61318	Y1731 delay timestamp is 0
CSCve89460	'cylon_mgr_F0-0.log' tracelog filing bootflash continously
CSCve60389	cylon_mgr crash
CSCve04262	Cylon_Mgr Crash in Adjacency Manager LoadBalance Get FID on Core Gigs Flaps SOAK
CSCvf08561	Cylon_Mgr Crash in Adjacency Manager Update FRR NextHop on Backup Core Gig Flap Soak
CSCvc27903	Part of data structure for MPLS labels missing
CSCvc20962	Port handle or Asic fwd handle becomes NULL for a LB Map object
CSCve25677	****MET ENTRYS EXHAUSTED ***** logs seen frequently
CSCve96485	IGMP snooping: Packet drops due to IGMP leave scenario in different BD
CSCvf09101	XE318SP3: Multicast hardening-S,G not formed after continuous clear ip mroute
CSCve61214	G8275.1: Master disqualified even though packets are flowign fine
CSCve36546	Unprotected Tracelogs Fix
CSCve06064	Packet drop on adding and deleting the vlans in Trunk EFP over 10G link.

Caveat ID Number	Description
CSCve95009	DATA traffic getting wrongly classified in H-QoS
CSCvd30613	Drop rate not calculated proper for parent polcy in HQoS with shaper apply
CSCvf14556	VLAN based egress classfication fails for incoming untagged frames; and for tagged frames with POP0
CSCvf39270	Generating a lot of "iomd_0-0.log" files saved in bootflash.
CSCvc76934	10G combo ports stop passing traffic when both ports has 1G Cu-sfp
CSCvd03480	Interfaces take a long time to come up with certain non Cisco SFPs
CSCvf36155	XE318 SP3 - VPLS traffic with LFA protection sees high loss when backup path is shut
CSCvc27889	Observing media type showing unkown on few reloads
CSCvf09882	IOMD ERR logs on auto-neg observed conitnuously which leads to bootflash space exhaustion
CSCvf52287	DOM not working for SFP-10G-LR from cisco-AVAGO vendor
CSCve24229	Fan Profile for TSOP and VCOP SSFP not working
CSCvf15605	Kernel core file generation not working
CSCvf30188	ONS-SE-Z1 is not recognized in tengig ports



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

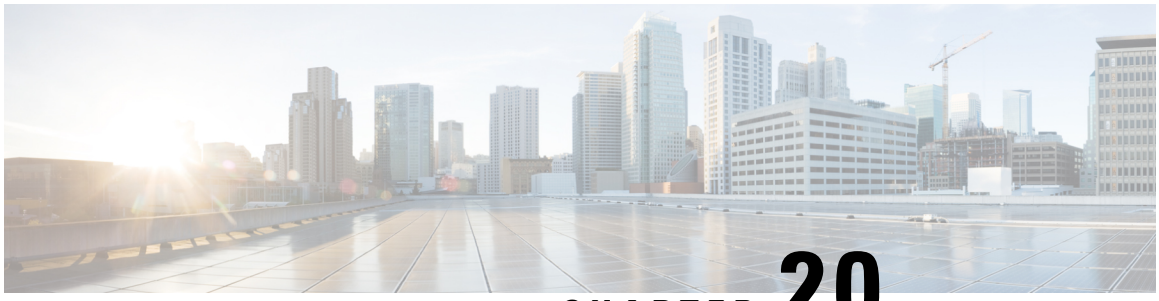
Cisco Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve effectiveness in network risk management and device troubleshooting. You can search for bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. For more details 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
CSCvb57842	Prompts to save configuration with no changes.

Resolved Caveats – Cisco IOS XE Release 3.18.1SP

Caveat ID Number	Description
CSCuz93695	Media-type unknown when the interface is in shut state.
CSCvb20923	ifStackTable populates different index values for EVC after reboot.



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

Identifier	Description