



Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE Fuji 16.9.x

First Published: 2019-03-21

Last Modified: 2020-10-05

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 1

- Cisco NCS 4201 and Cisco NCS 4202 Overview 1
- Feature Navigator 2
- Hardware Supported 2
- Determining the Software Version 2
- Bundled FPGA Versions 2
- Limitations and Restrictions on the Cisco NCS 4201 and Cisco NCS 4202 Series 3
 - Important Notes 4
 - Field Notices and Bulletins 4
 - MIB Support 4
 - Accessibility Features in the Cisco NCS 4201 and Cisco NCS 4202 Series 4

CHAPTER 2

New Features 5

- New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.7 5
- New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.7 5
- New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.6 6
- New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.6 6
- New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.5 6
- New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.5 6
- New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.4 6
- New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.4 6
- New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.3 7
- New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.3 7
- New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.2 7
- New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.2 7

New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.1a	7
New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.1a	8

CHAPTER 3**Caveats 9**

Cisco Bug Search Tool	10
Open Caveats – Cisco IOS XE Fuji 16.9.7	10
Platform Independent Open Caveats – Cisco IOS XE Fuji 16.9.7	10
Resolved Caveats – Cisco IOS XE Fuji 16.9.7	10
Platform Independent Resolved Caveats – Cisco IOS XE Fuji 16.9.7	10
Open Caveats – Cisco IOS XE Fuji 16.9.6	11
Platform Independent Open Caveats – Cisco IOS XE Fuji 16.9.6	11
Resolved Caveats – Cisco IOS XE Fuji 16.9.6	11
Platform Independent Resolved Caveats – Cisco IOS XE Fuji 16.9.6	11
Open Caveats – Cisco IOS XE Fuji 16.9.5f	12
Resolved Caveats – Cisco IOS XE Fuji 16.9.5f	12
Open Caveats – Cisco IOS XE Fuji 16.9.5	12
Resolved Caveats – Cisco IOS XE Fuji 16.9.5	12
Platform Independent Resolved Caveats - Cisco IOS XE Fuji 16.9.7	13
Open Caveats – Cisco IOS XE Fuji 16.9.4	14
Resolved Caveats – Cisco IOS XE Fuji 16.9.4	14
Open Caveats – Cisco IOS XE Fuji 16.9.3	15
Resolved Caveats – Cisco IOS XE Fuji 16.9.3	15
Open Caveats – Cisco IOS XE Fuji 16.9.2	15
Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.2	16
Resolved Caveats – Cisco IOS XE Fuji 16.9.2	17
Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.2	17
Open Caveats – Cisco IOS XE Fuji 16.9.1a	19
Resolved Caveats – Cisco IOS XE Fuji 16.9.1a	22



CHAPTER 1

Introduction



- Note** Explore the [Content Hub](#), the all new portal that offers an enhanced product documentation experience.
- Use faceted search to locate content that is most relevant to you.
 - Create customized PDFs for ready reference.
 - Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience. Do provide feedback about your experience with the Content Hub.

This document provides information about the IOS XE software release for the Cisco NCS 4201 and Cisco NCS 4202 beginning with Cisco IOS XE Release 3.18SP.

- [Cisco NCS 4201 and Cisco NCS 4202 Overview, on page 1](#)
- [Feature Navigator, on page 2](#)
- [Hardware Supported, on page 2](#)
- [Determining the Software Version, on page 2](#)
- [Bundled FPGA Versions, on page 2](#)
- [Limitations and Restrictions on the Cisco NCS 4201 and Cisco NCS 4202 Series, on page 3](#)
- [Field Notices and Bulletins, on page 4](#)
- [MIB Support, on page 4](#)
- [Accessibility Features in the Cisco NCS 4201 and Cisco NCS 4202 Series, on page 4](#)

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

NCS4201 is a fixed router and does not have any field replaceable units.

The following table lists 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
	1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 ports T1/E1 + 4 ports T3/E3	NCS4200-3GMS
	8-Port 1GE RJ45 and 1-Port 10GE SFP+ module	NCS4200-1T8LR-PS

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.
- To downgrade from Cisco IOS XE Fuji 16.9.x release, always use a lower version of the ROMMON. If you downgrade with ROMMON version 15.6.(24r)S, it may result in a continuous boot loop and might crash. This is applicable to the Cisco NCS 4201 and NCS 4202 Series variants.
- 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.

Important Notes



Note Port channel 61-64 is not supported in the 16.9.3 release. The range of configurable port channel interfaces has been limited to 60.

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

This chapter describes the new hardware and software features supported on the Cisco NCS 4200 Series in this release.

- [New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.7, on page 5](#)
- [New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.7, on page 5](#)
- [New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.6, on page 6](#)
- [New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.6, on page 6](#)
- [New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.5, on page 6](#)
- [New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.5, on page 6](#)
- [New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.4, on page 6](#)
- [New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.4, on page 6](#)
- [New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.3, on page 7](#)
- [New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.3, on page 7](#)
- [New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.2, on page 7](#)
- [New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.2, on page 7](#)
- [New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.1a, on page 7](#)
- [New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.1a, on page 8](#)

New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.7

There are no hardware features for this release.

New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.7

There are no software features for this release.

New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.6

There are no hardware features for this release.

New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.6

There are no software features for this release.

New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.5

There are no hardware features for this release.

New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.5

There are no software features for this release.

New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.4

There are no hardware features for this release.

New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.4

- **SNMP Dying Gasp Support**

The SNMP Dying Gasp is supported on the NCS 4201 and 4202 series routers through FPGA:

The maximum number of supported SNMP servers for SNMP Dying Gasp is 2 and the maximum number of supported Link-OAM Dying Gasp is 6.

For more information, see the Cisco NCS 4200 Series Software Configuration Guide, Cisco IOS XE Fuji 16.9.x.

New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.3

There are no new features introduced for this release.

New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.3

- **BDI statistics Support on RSP3 Module**

Starting Cisco IOS XE Fuji Release 16.9.3, BDI statistics is supported on the RSP3 module. The **show interface** command displays the BDI statistics for the interface.

For more information, see [Carrier Ethernet Configuration Guide, Cisco IOS XE Fuji 16.9.x \(Cisco ASR 4200 Series\)](#)

- **Storm Control Support on Port Channel on RSP3 Module**

Starting with Cisco IOS XE Fuji 16.9.3, storm control over port channel is supported on the RSP3 module. Storm control over port-channel is applicable for port channel interfaces, and is used for restricting the unicast, broadcast and multicast ingress traffic on the port channel interfaces.

For more information see, [Storm Control Configuration Guide, Cisco IOS XE Fuji 16.9.x \(Cisco ASR 4200 Series\)](#)

New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.2

There are no new features introduced for this release.

New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.2

There are no new features introduced for this release.

New Hardware Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.1a

There are no new hardware features in this release.

New Software Features for NCS 4201 and NCS 4202 in Cisco IOS XE Fuji 16.9.1a

• HDLC or PPP to Ethernet IPv4 Interworking Pseudowire

The L2VPN interworking allows you to connect disparate attachment circuits, for example, TDM and Ethernet attachment circuits. The L2VPN interworking operates in IP (routed) mode that facilitates transport of IPv4 payload in HDLC or PPP frames to Ethernet, over MPLS network translation. The configuration is supported on NCS4200-3GMS.

For more information, see the [1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.9.x \(Cisco NCS 4200 Series\)](#).

• MPLS TE and BGP PIC Edge

MPLS TE Load balancing, BGP PIC Edge, and RFC 3107 are now supported over TE-FRR.

For more information on the feature, see the [IP Routing: BGP Configuration Guide, Cisco IOS XE Fuji 16.9.x](#).

• RS232 Sync

The serial interface module now supports pseudowire transport over MPLS and raw socket for Sync traffic. Out of 14 ports, 6 ports (8-13) support sync interfaces. RS232 Sync data is carried over Raw Socket.

For more information, see the [Cisco NCS 4200 Series Software Configuration Guide, Cisco IOS XE Fuji 16.9.x](#).

• Support for STS1e

3GSM-DS3 ports and 48 T3/E3 ports can be configured in STS-1e mode.

For more information, see the [48-Port T1/E1 CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.9.x \(Cisco NCS 4200 Series\)](#) and [1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module Configuration Guide, Cisco IOS XE Fuji 16.9.x \(Cisco NCS 4200 Series\)](#).

• Programmability Support

- Candidate Configuration—A temporary configuration that can be modified without changing running configuration. You can then choose when to update the device's configuration with the candidate configuration, by committing and confirming the candidate configuration.
- Model-Driven Telemetry—Model-driven telemetry allows network devices to continuously stream real time configuration and operating state information to subscribers.

For more information, see the [Programmability Configuration Guide, Cisco IOS XE Fuji 16.9.x](#).

• VRRPv3 SNMP MIB

SNMP MIBs are now supported for Virtual Router Redundancy Protocol (VRRP) version 3. For more information on the supported MIBs, see the [First Hop Redundancy Protocols Configuration Guide, Cisco IOS XE Fuji 16.9.x \(NCS 4200 Series\)](#).



CHAPTER 3

Caveats

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

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

The bug IDs are sorted alphanumerically.



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

- [Cisco Bug Search Tool, on page 10](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.7, on page 10](#)
- [Platform Independent Open Caveats – Cisco IOS XE Fuji 16.9.7, on page 10](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.7, on page 10](#)
- [Platform Independent Resolved Caveats – Cisco IOS XE Fuji 16.9.7, on page 10](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.6, on page 11](#)
- [Platform Independent Open Caveats – Cisco IOS XE Fuji 16.9.6, on page 11](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.6, on page 11](#)
- [Platform Independent Resolved Caveats – Cisco IOS XE Fuji 16.9.6, on page 11](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.5f, on page 12](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.5f, on page 12](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.5, on page 12](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.5, on page 12](#)
- [Platform Independent Resolved Caveats - Cisco IOS XE Fuji 16.9.7, on page 13](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.4, on page 14](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.4, on page 14](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.3, on page 15](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.3, on page 15](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.2, on page 15](#)
- [Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.2, on page 16](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.2, on page 17](#)

- [Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.2, on page 17](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.1a, on page 19](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.1a, on page 22](#)

Cisco Bug Search Tool

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

Open Caveats – Cisco IOS XE Fuji 16.9.7

There are no open caveats for this release.

Platform Independent Open Caveats – Cisco IOS XE Fuji 16.9.7

Caveat ID Number	Description
CSCvv79677	ASR902-RSP2 crashed after BGP flaps
CSCvv80471	IPv6 BGP update is not applied after changes to inbound route-map
CSCvw19062	Changing external route tag does not update origin code in BGP
CSCvw44599	IPSLA UDP-jitter: Packets are sent at appx 2ms less or more than the config packet interval

Resolved Caveats – Cisco IOS XE Fuji 16.9.7

Caveat ID Number	Description
CSCvv42595	REP flapping randomly and frequently due to port down

Platform Independent Resolved Caveats – Cisco IOS XE Fuji 16.9.7

Caveat ID Number	Description
CSCvu85572	Dynamic neighbor does not form when peer-group is shutdown in different vrf
CSCvv17560	BMP BGP server can lead to CPUHOG and crashes

Caveat ID Number	Description
CSCvv40006	Traceback: IP SLA triggers INJECT_HDR_LENGTH_ER and INJECT_FEATURE_ESCAPE log message
CSCvv64633	BGP: advertised community list is malformed due to GSHUT community
CSCvw05035	BGP fall-over not working when Null0 static route is configured
CSCvw37109	Pseudowire interface may be unexpectedly removed from VFI on unrelated configuration change
CSCvx02515	BGP IPv6 link-local session does not come up

Open Caveats – Cisco IOS XE Fuji 16.9.6

Caveat ID Number	Description
CSCvt21903	Traffic drops observed with IPSec traffic
CSCvt82525	Crash while IPV6 updating prefixes
CSCvv16454	Traffic failure due to MPLS ECMP load-balancing in one of the labelled path

Platform Independent Open Caveats – Cisco IOS XE Fuji 16.9.6

There are no platform independent open caveats for this release.

Resolved Caveats – Cisco IOS XE Fuji 16.9.6

Caveat ID Number	Description
CSCvq07399	OBFL updation with valid time after NTP Sync in RTC failure case
CSCvt25458	MPLS TE is not coming UP when bandwidth configured on Juniper head end

Platform Independent Resolved Caveats – Cisco IOS XE Fuji 16.9.6

Caveat ID Number	Description
CSCvs18780	SR Labels not installed in forwarding plane when there are multiple sources for the prefix SID

Caveat ID Number	Description
CSCvs95815	C1111 telnet refused for link-local addresses when using ipv6 access class

Open Caveats – Cisco IOS XE Fuji 16.9.5f

Caveat ID Number	Description
CSCvn55871	T1 serial interface went down with encapsulation mode as PPP with remote loopback config as iboc.
CSCvs64478	VTY configuration changed transport input protocols

Resolved Caveats – Cisco IOS XE Fuji 16.9.5f

Caveat ID Number	Description
CSCvr97004	VTY lines higher than 5 cannot be configured NVGEN
CSCvt21903	Traffic drops observed with IPSec traffic

Open Caveats – Cisco IOS XE Fuji 16.9.5

Caveat ID Number	Description
CSCvn55871	T1 serial interface went down with encapsulation mode as PPP with remote loopback config as iboc.
CSCvs64478	VTY configuration changed transport input protocols

Resolved Caveats – Cisco IOS XE Fuji 16.9.5

Caveat ID Number	Description
CSCvr61371	BFD remains down when using PBR on BDI/interface

Platform Independent Resolved Caveats - Cisco IOS XE Fuji 16.9.7

Caveat ID Number	Description
CSCvf02131	IP SLA can trigger crash when used with MPLS probe
CSCvm79556	RSP3: MSPW VC down after Switchover (Error Local access circuit is not ready for label advertise)
CSCvo55194	After RSP switchover label imposition was not programmed in Software on APS standby router
CSCvo71904	The 'app-hosting' fails with "ip unnumbered" configuration in Virtual PortGroup
CSCvp74674	QoS fails to apply to tunnel2 when underlying tunnel1 reachability change
CSCvp77521	Device-tracking tracking 0.0.0.0 mask ignored after Legacy IPDT to SISF conversion
CSCvp81958	BGL18 Alpha: Cat9x00 hitting "No connections to Shell Manager available for processing the command"
CSCvp91484	CSCvp91484 - SDA Fabric Multicast - Unable to calculate RPF from LISP
CSCvq19669	Evaluation of all for TCP_SACK
CSCvq33994	BGP YANG oper address-family fails with vpv4-unicast
CSCvq56114	Cat3k crash in IGMP code due to invalid source count in DNS lookup
CSCvq58265	ASR1K BGP PIC Repair path broke after link flap
CSCvq69866	HSRPv2 crash whilst retrieving group from received packet
CSCvq70148	BGP is improperly formatting the BGP ASSET attribute if ASSET attribute length is beyond 255
CSCvq76305	ASR900 autoRP listener functionality issue
CSCvq78692	mGRE L3VPN broken after reload
CSCvq89252	IP SLA for Path-Jitter returning a value which isn't defined by the MIB
CSCvq96794	VPLS label misprogramming after RSP switchover
CSCvr05213	Smart licensing PID and SN logs filling up the IOSRP tracelogs
CSCvr05406	LISP Map-cache not updated correctly after wired Host-mobility
CSCvr08740	Router crash after receiving EVPN route-type 2 without any ext-community
CSCvr09014	IGP metric not detected MPLS TE topology

Caveat ID Number	Description
CSCvr10897	Adjacency SIDs not detected in mpls traffic-eng topology (interop issue)
CSCvr12450	LISP: Block adding SVI (anycast gateway) MAC address to LISP ethernet database after svi reconfig
CSCvr18919	Cat9k SVL - Upon redundancy failover, route being purged on downstream device
CSCvr23104	BGP looped update among 3 peers
CSCvr27393	Crash on "BGP Router" process
CSCvr37065	C9200L kernel Oops jumbo packets
CSCvr39868	Unexpected reload when issueing show ip mroute vrf <vrf> verbose
CSCvr40112	Removing pseudowire-class for 1 peer makes all the peers fail.
CSCvr54031	TBs seen with scaled IP SLA configs with "ip sla reset"
CSCvr59231	Cat9400- PNP fails with Dual Supervisor with non default startup vlan
CSCvs02038	BGP Loss of RPKI Table
CSCvs15811	cbr8/L2VPN : Toggle of PW-Status-TLV causes Backup PW to remain DOWN

Open Caveats – Cisco IOS XE Fuji 16.9.4

Caveat ID Number	Description
CSCvo19770	Router crashes at hashtable_get_nth_entry
CSCvp24919	ToD UBX Format - Incorrect header and checksum calculation are noticed
CSCvq01602	After IPv6 nd cache expires, transit traffic fails when ECMP is performed

Resolved Caveats – Cisco IOS XE Fuji 16.9.4

Caveat ID Number	Description
CSCvm06775	ATOM CW is not exchanged after node reload
CSCvm46312	ASR920: CFM remote endpoint with backup pseudowire points to primary peer IP in HSPW
CSCvn01354	ICMP echo probe is successful when the source interface does not have the IP address
CSCvo21122	Memory leak is observed at hman process
CSCvo35275	ASR-920:MVPN: Unable to pass high MTU multicast packets-MDT-MTU

Caveat ID Number	Description
CSCvo41879	Interface is not joined to mcast map-notify after reload
CSCvo62584	DHCP discover packets are dropped at firewall since UDP source port is set as 0
CSCvo67856	The in.telnetd process consumes 100% CPU in show process
CSCvo90060	Wrong label programming leads to traffic drop
CSCvo90231	Spurious accesses are seen in show alignment output with BGP
CSCvp71303	Router crashes when tod-clock revertive command is executed
CSCvp78236	Router crashes during SNMP configuration, ospfv3_pdb_from_router_info

Open Caveats – Cisco IOS XE Fuji 16.9.3

Caveat ID Number	Description
CSCvj32802	Tunnel stats are not working after FRR cutover
CSCvm76770	Unpredictable asymmetry on T1/E1 IM
CSCvn99716	C3794 controller displays down state with traffic flow
CSCvp34829	Portchannel 61-64 is not supported in 16.9.3

Resolved Caveats – Cisco IOS XE Fuji 16.9.3

Caveat ID Number	Description
CSCvk72044	16101: cylon_mgr crash@adjmgr_get_fid_index seen in soak run on 27th Sep 16.10.1 image
CSCvn49741	ASR903/920 cylon_mgr crash.
CSCvn64973	A900-IMA4OS module reload with controller mode change
CSCvo07619	ASR920-BDI IPv6 ping failure_FMFP_OBJ_Download_Failure

Open Caveats – Cisco IOS XE Fuji 16.9.2

Caveat ID Number	Description
CSCvi91056	ALARM_SYNC_FAIL alarm seen with slave Phase Aligned and sync packets are incrementing <167>

Caveat ID Number	Description
CSCvj86475	HS1: time-stamp engine stats are very slow and it is not showing at right port.
CSCvk73179	ASR920: TDM traffic in priority queue affected with 9,000 bytes size packet of transit data traffic
CSCvm21736	The negotiation auto configuration gets removed from dual rate ports post node Hard reset/Power cycle
CSCvm41478	Last reload reason seen as "Reload command" after upgrade to V169 from 316.7 CCO
CSCvm84084	SVSP-279 - NCS4202 EVC egress policy shows drop rate counters as 0
CSCvm05115	High reconvergence of 2 seconds in case of local failover recovery on hot-spring
CSCvm16466	Ping fail over EVC Local Connect circuit (arp request getting dropped)
CSCvm97580	On shutting backup ABR, traffic drops observed for 6PE over primary ABR drops
CSCvk77003	One VLAN traffic is not flowing in scaling BCPoMLPPP with 64 VLANs
CSCvm08992	E1 interfaces go DOWN on remote alarm (RDI)

Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.2

Caveat ID Number	Description
CSCvj17588	Router may reload in BGP Router process when interface flap occurs with IPv6 MPLS per vrf routes
CSCvk59169	Strict SID has NOT been enabled in ISIS segment-routing
CSCvm52543	Subscriber session hangs after the upgrade and reload
CSCvm59483	Host crashes the DSP if ipv6 commands are configured under Service-Engine [Purge ipv6 config option]
CSCvm61279	Crash under AFW_application_process with shared-line configuration
CSCvm76590	CUBE does not forward 200 OK in SRTP-RTP scenario with TCL script on Dial-peer
CSCvm76699	TCP closed when using Virtual IP HA(high availability)setup with WSAPI registration
CSCvn01507	ISR not recalculating the hash value correctly after payload change
CSCvn02047	Configuring more than 5k NAT entries cause high CPU utilization with no traffic.

Resolved Caveats – Cisco IOS XE Fuji 16.9.2

Caveat ID Number	Description
CSCvj69014	Interface flap issues in ASR920 register in ES5
CSCvj76129	Hotspring1: license status not shown for 1588 feature
CSCvk05865	AIS: box crashed at zl303xx_AprRemoveServer
CSCvk07103	HS1-V169: REFSYNC pair is not getting removed while moving from 75.1 Master to default BC
CSCvk28844	HS1: Kernel MMI Read Crash on Enabling IP SLA and PTP
CSCvk73145	ASR920: PTP flap between PHASE ALIGNED and FREQUENCY LOCK with 9,000 bytes data packets in transit
CSCvj76560	ASR920:BFD DDR BUSY condition not recovered
CSCvk07069	ASR920:OBFL logging for SBE/MBE FPGA interrupts
CSCvk62834	16101:cylon_mgr crash@nile_cef_prefix_v4u_get_adj_info seen in soak run on 16th July Polaris image
CSCvk00584	Ethernet SLA tracking not working for Xconnect UP mep sessions (DMM/1DMM)
CSCvh67635	Onboard option missing for show logging CLI
CSCvj70711	ASR920: BFD flap during DDR3 Busy recovery
CSCvk45460	ASR920 MLDP:Router crashed after breaking the core link with recursive enabled
CSCvm21116	ASR920:RP-reset when show pla har pp act commd is executed for the failed object after EMPLSintd exhaust
CSCvi91527	RSP2 8xT1E1 Adaptive Clock Recovery in UNKNOWN status
CSCvj22030	ACR fails with +/- 50 ppm tolerance
CSCvk23983	DATAINCONSISTENCY observed with VFI and XCONNECT configuration during reload

Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.2

Caveat ID Number	Description
CSCuz14861	IOS-XE Fails to correctly populate RTCP SSRC Field
CSCvf65079	ASR CUBE 1K reloaded with reason: RG-application reload on voice-b2bha RG

Caveat ID Number	Description
CSCvj16209	CME with external SIP trunk registration results into crash
CSCvj24940	Voice VRF with No Bind OPTIONS Ping response not sent
CSCvj25678	Crash after failing to modify xcode
CSCvj27172	Crash during Generic Call Filter Module cleanup
CSCvj43156	Crash in XDR process: "fib_rp_table_broker_encode_buf.size <= FIB_RP_TABLE_BROKER_ENC_BUF_SZ"
CSCvj50005	ISR4K PPE ucode crash when processing ipsec traffic on CWS tunnel
CSCvj69654	OSPF originates default route without "default-information originate"
CSCvj73544	OSPF routing loop for external route with multiple VLINKs/ABRs
CSCvj88138	VASI NAT: FTP ALG translation is sometimes failed
CSCvj91448	PKI:-IP address parsing issue while printing the subject name if classless IP is used in Trustpoint
CSCvj92548	CSR1k-FlexVPN: Spoke to Spoke: Implicit NHRP entry due to expired resolution request handling.
CSCvj92862	Router returns 255 length byte-stream chars instead of actual length for OSPFV2 Key-string
CSCvj95351	OSPF SR uloop : After issuing clear ip ospf process OSPF process crashed.
CSCvk00446	BGP high CPU when config 256k vxlan static route
CSCvk02072	Hoot-n-holler multicast traffic marked with DSCP 0
CSCvk07838	CUBE is using wrong source IP address to send SIP error
CSCvk10633	BGP crash while running show command and same time BGP peer reset
CSCvk12152	Unable to remove command ip nat inside destination
CSCvk15062	Modification to ZBFW access-lists do not reflect in TCAM
CSCvk17777	When using VRF NAT port used for ftp data is not freed
CSCvk24323	Router crash in ISIS with SR Ti-LFA
CSCvk27007	MGCP status remains Down after IOS upgrade caused by CSCvh70570
CSCvk37875	High Availability system with two Voice Gateways - Crash
CSCvk49905	Crash when shifting the layer 2 LACP member peer from one link to another
CSCvk53405	Router crash - AFW_application_process

Caveat ID Number	Description
CSCvk56331	Initial contact in IKEv1 phase 2 rekey (QM1) causes all crypto sessions to drop
CSCvk60184	Random crash of data plane with SRTP-SRTP / SRTP-RTP load tests
CSCvk65072	Crash due ZBF + NAT
CSCvk65354	Extension Mobility Not working when used with Greek locale on SIP CME
CSCvk66880	CUBE incorrectly fomats SIP SDP
CSCvk69075	No calls shown in output show call active voice brief on CUBE & stale entries are present
CSCvk69093	CUBE is not responding to SIP INFO
CSCvm01351	Observed IPv6 Adj memory leaks
CSCvm02627	Incorrect Contact port 5060 used instead of 5061 by CUBE in 302 Moved Temporarily message
CSCvm03744	%FMFP-3-OBJ_DWNLD_TO_DP_FAILED:fman_fp_image:xxx" appears when configured ip port-map on Router
CSCvm06270	ICMP unreachables are not sent to the client on C1117 platform
CSCvm08571	Rework need on CSCvj59170 to support SDP parsing
CSCvm16619	CPP-mcplo-ucode crash while encrypting SIP packets with ALG NAT for SIP
CSCvm53491	SIP CME Crashes when Calling Shared Line
CSCvm56592	CME/BE4K: Corrupted config file for Auto Registered IP Phones after reload
CSCvm56670	ACL dropping packets after updating it - %CPPEXMEM-3-NOMEM
CSCvm66103	Crash due to communication failure - IPC (Inter-Procedure Call) messages between DSP and RP.

Open Caveats – Cisco IOS XE Fuji 16.9.1a

Caveat ID Number	Description
CSCvg00947	Serial IM LEDs shows inconsistent behavior while performing SSO
CSCvg66190	IOT: Rawsocket disconnected clients are not sending any notification
CSCvh51488	RS232 sync, when continous traffic is sent without interframe gap, RX<TX with end to end traffic
CSCvh83686	BGP Link Bandwidth community gets corrupted for a large values

Caveat ID Number	Description
CSCvi11914	BGP PIC/Max-paths:150K scale device stuck with pending issues for huge time with network changes
CSCvi12438	Media-info,status, oper-config fields wrong in port phy status command
CSCvi72770	Unpredictable asymmetry across the port on C37.94 IM
CSCvi84049	Attaching E1 serial interface with multilink group failed
CSCvi90526	OSPF TILFA: SRLG protect tilfa path computation ALGORITHM fails due to wrong directly connected flag
CSCvi91056	ALARM_SYNC_FAIL alarm seen with slave Phase Aligned and sync packets are incrementing <167>
CSCvi91527	RSP2 8xT1E1 Adaptive Clock Recovery in UNKNOWN status
CSCvi92837	Cli "show ptp port running" showing 187 clock class and its own clock identity <Polaris>
CSCvi92979	ISIS SRTE: verbatim tunnels stay UP even if the IGP is shut (happens after fail over)
CSCvj02225	RS232 rawsocket (async/sync) failing due to punt issue in datapath
CSCvj05503	Channelized T3 function is setting DS2 X bits to 0 for normal condition
CSCvj09305	Slow convergence when configuring ha-mode sso for IPv6 peers
CSCvj10061	Display full IPv6 address in "sh l2tp tunnel"
CSCvj11220	UDLD Err Disable (Admin down) observed on migration from customer v155 to v166 label .
CSCvj16369	Alarm is not asserted when we do no mode and mode on vt1.5 and ct3 with alarm injected (arrive)
CSCvj22030	ACR fails with +/- 50 ppm tolerance
CSCvj24884	Traceback seen while loading image in Active and standby
CSCvj35547	[HS] : 2 way time error drifts 1 us in just 15-20 minutes after locking 23 hours to PL
CSCvj40597	show ptp port running and detail showing incorrect clock IDS.
CSCvj41841	MPLS TTL decremented during PHP process on ASR920
CSCvj49266	Rx getting dropped at Master after losing its 10M input.
CSCvj60860	RS232 Async serial interface output stats are not incr and no end to end traffic.
CSCvj67071	RS232 Async: line and pattern issues in Albedo with different data/stop bits.
CSCvj70563	Higher latency with E&M traffic

Caveat ID Number	Description
CSCvj72171	PPPoE packets (PADI PADO PADR PADS PADT) counters are not getting incremented after SSO
CSCvj73841	Overly aggressive initial SPF delay timer is configured -> SR uloop does not take effect
CSCvj74325	X.21: Serial IM flaps/hangs when CEM interface allows to config clock rates 4032000 and 8064000.
CSCvj78075	SAP: YANG: Yang model for arp entries is missing arp alias support
CSCvj81382	IPv6 AAA Prefix Support for 3rd party PPP clients no password for -dhcpx6 Access-Request
CSCvj82372	CPUHOG observed when rs232 aync raw-socket config and unconfig on ASR920.
CSCvj82885	IOS thread disabled interrupt Tracebacks seen with r232 async session
CSCvj84567	RS232 sync: multiple session establishment failures leads to event memory exhaustion in clients
CSCvj84662	ENM IM: Frame and Pattern errors see with Type TO in default operation mode(2-wire).
CSCvj85608	ARP reply not accepted if sourced from nat alias address in other VRFs
CSCvj86932	X21: CEM ingress and Egress counters are not incrementing for different clock rates.
CSCvj88449	VCoP BERT test to a physical loop
CSCvj89265	IOT: Issue with duplex mode while creating RS422 Service
CSCvj93060	VRF stuck in deletion mode
CSCvj99066	Mgmt Port Duplex(right) LED is off even port in duplex full state
CSCvk00980	Router crashed while configuring Async raw-tcp service post OIR.
CSCvk23646	RS232 - traffic fails with parity values except default
CSCvk23733	RS232 Async: Pattern(SLIP) issues seen with higher raw-socket packet-length values(>510)
CSCvk24323	ASR920 crash in ISIS with SR Ti-LFA
CSCvk30191	RS232 async raw-socket: IM rebooted and IFCFG_CMD_TIMEOUT traces seen with OIR.
CSCvk31981	RS232 async: raw TCP sessions are up even tough cable is not connected.
CSCvk32822	QoS stats process crash
CSCvk14335	LMM counters are not getting updated by SSFP - UP/DOWN direction
CSCvk28844	Kernel MMI Read Crash on Enabling IP SLA and PTP

Caveat ID Number	Description
CSCvk32072	Down MEP SLA status showing as 0
CSCvk56760	10M remains in lock state and REF remains OK even after cable pull
CSCvk60607	kernel crash on soak with mac learning /clear
CSCvk49930	GNSS LED behaviour is not as per the specifications
CSCve01696	Support IPsec feature with metroipaccess license.

Resolved Caveats – Cisco IOS XE Fuji 16.9.1a

Caveat ID Number	Description
CSCuy30367	ENH: IOS-XE should allow "ip address dhcp" on Tunnel interfaces
CSCvd81332	EVENTLIB-3-CPUHOG: SIP1: iomd traceback observed while doing SSO
CSCve05859	Exxx EIN: G.8275.1 testing: Clock loop forming between sync and ptp
CSCve16000	Max of ECMP path to 8
CSCve57194	Crashes @ fillin_mempool_pc_array, mempool_pc_summary_tty
CSCve75491	TE auto-bw: Incorrect bandwidth requested on soaking with traffic
CSCvf05560	Conditional EXP Marking for BDI+EVC
CSCvf45581	QoS: Configuration failed. Can not configure more than one access-group per class
CSCvf50635	Dynamic stream are getting deleted on ASR920 router with G8275.2 profile <POLARIS> ASR920 Timing THS
CSCvf66442	MPLS IP support over Routed VPLS.
CSCvf67781	IOT: In SERIAL controllers, the clock-rate value 128000 is not shown in 'show running-config all'
CSCvf72306	Placeholder to support multiple EFPs per port with BDI
CSCvf80056	MAC-FLAP-Syslog-Not generated for TEFP BDs
CSCvf82663	RSP3C crashed at dl_callback
CSCvf90662	doing configure replace of async config with cem config blocks all configs on interface
CSCvf90832	UTC Offset is NOT taken care properly when VP is selected.
CSCvf90854	configured priority2 under ptp clock is not sent downstream when T- BC selected VP
CSCvf91208	Unable to retrieve stream with G8275.2 profile <POLARIS> ASR920 Timing THS

Caveat ID Number	Description
CSCvf96793	DS3 VCOP AIS raised for J1 byte mismatch
CSCvg01156	G275.2 Huge TIE jump seen on slave after reload completes on master
CSCvg04717	DDR Busy and Calibration handling in FPGA software driver
CSCvg06691	G8265.1: huge TIE deviation while master is lost and regained continuously.
CSCvg08224	G8265.1: PTP flaps between HOLDOVER and LOCKED with 64/64 packet rate and HOTSTANDBY
CSCvg14825	Require varbind entSensorPrecision,Scale & Type along with trap entSensorThresholdNotification
CSCvg21913	AMS port netsync is not up on reload
CSCvg23956	VPLS Backup PW: Enable member bdi CLI under l2vpn xconnect context
CSCvg25003	Router gets rebooted with PTP master switch
CSCvg28721	Uea-mgr crashed while trying to install a label entry in kbp(update case)
CSCvg38326	To throw warning and reject the priority configuration in class-default
CSCvg42691	P node ECMP loadbalancing failing for ip traffic
CSCvg51358	DHCPNAK is not sent in roaming scenario.
CSCvg65763	TOD cisco format got broken.
CSCvg66293	IOT: Admin and Oper state of C37.94 controller are not proper in SNMP IfTable
CSCvh04843	G.8275.1: Unable to scale the number of ports beyond 8.
CSCvh14208	920-TDM-OCX : Automatic EEPROM Update required
CSCvh41614	IoT[T1E1 CAS]: CEM counters are getting zero after delete/recreate cem-group with CAS
CSCvh57050	IGMP multicast SSM-map with DNS doesn't work with IGMPv3
CSCvh57360	Traceback seen in ASR920 TDM THS tb
CSCvh60871	Unexpected Reboot following 'show platform software adjacency oce [ID]'
CSCvh61453	NULL remote_hostname from LAC
CSCvh67138	RS232 sync, when "no chan-group" is done sessions are not getting removed
CSCvh69518	%SYS-3-TIMERNEG:Cannot start timer with negative offset Process= "ARP Background"
CSCvi31493	Configuration of BGP auto-summary using NETCONF fails

Caveat ID Number	Description
CSCvi36351	standby rp crash on removing member link from port-channel
CSCvi60900	DHCP Leasequery Padding contains previously used data
CSCvi79409	ENM flaps/hangs on configuring CEM interface
CSCvi80618	G.8265.1- SYNC and Delay Request are not being injected at ASR920 with VRF.
CSCvi95085	PTP Holdover Timer resets to zero as soon as QL Flap in the event of double failure
CSCvi97136	Stream is still active though the clock port deleted at master.
CSCvi97402	Conditional marking not working for new policy-map when all 3 marker profile are used
CSCvj02290	Sync RS232: router reloads when traffic is sent in both directions simultaneously
CSCvj04138	"show ptp port virtual" showing Signal Fail as True eventhough the port is up
CSCvj04207	PTP over IMA8Z and IMA2Z is not working
CSCvj06628	With HSRP Loop ,Unicast ARP Packet drops due to Br Q choke
CSCvj28545	RS422 service is not working on ports 0 to 3
CSCvj39051	Default clock class 6 without input 1pps config <169>
CSCvj39606	AG1 CLI command "show ptp port running detail" not showing output
CSCvj40006	Adding one more vlan tag to the existing service instance causing entire traffic dr
CSCvj43887	Type TO is not working for different payload sizes
CSCvj53263	IOT: Issue with Raw Socket Packet length default value
CSCvj63480	RS232 Async: IOSXE-WATCHDOG - Router crashed while performing OIR
CSCvj65555	G8275: Clock class value is 6 even when TOD is removed in TGM
CSCvj67071	RS232 Async: line and pattern issues in Albedo with different data/stop bits.
CSCvj69889	Memory leaks seen when sync RS232 raw-socket service is unconfigured and re-configured
CSCvj70809	%SPA_SERIAL_IM-3-NULL_DATA_STRUCTURE: NULL pointer detected: msg in set destination address
CSCvj85141	Policy-map on Multilink interface interrupts ARP
CSCvj87392	DHCP server with option 249 pushes only the routes configued in the first instance.
CSCvj89265	IOT: Issue with duplex mode while creating RS422 Service
CSCvk20144	Not able to see the physical-layer configuration under "show run" command

Caveat ID Number	Description
CSCvk32660	EM IM: Dejitter Buffer Not Taking Effect on IM or Router Bootup
CSCvh55384	Need to accept user configurable 4-Wire E and M CEM payload and dejitter buffer values

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 NON-INFRINGEMENT 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)

© 2019 Cisco Systems, Inc. All rights reserved.

