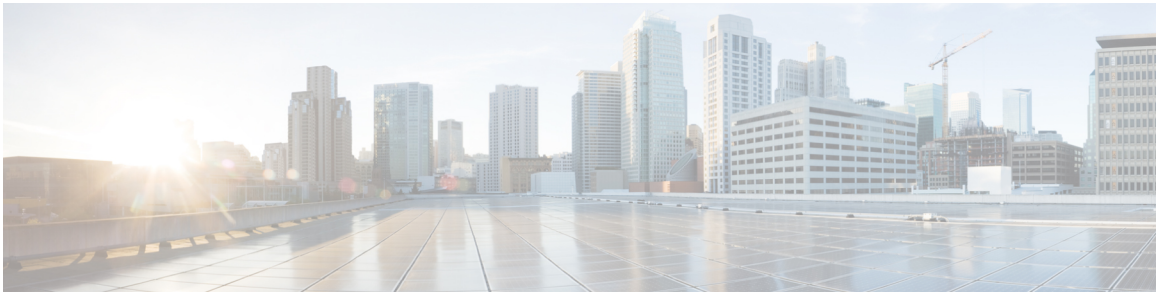


Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS XE Cupertino 17.9.x

First Published: 2022-08-01

Last Modified: 2026-04-30

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

Supported Hardware 1

Cisco Catalyst 9200 Series Switches—Model Numbers 1

Network Modules 4

Optics Modules 4

CHAPTER 2

Whats New in Cisco IOS XE Cupertino 17.9.x 5

Whats New in Cisco IOS XE Cupertino 17.9.9 5

Whats New in Cisco IOS XE Cupertino 17.9.8 5

Whats New in Cisco IOS XE Cupertino 17.9.7 5

Whats New in Cisco IOS XE Cupertino 17.9.6a 5

Whats New in Cisco IOS XE Cupertino 17.9.6 6

Hardware Features in Cisco IOS XE 17.9.6 6

Software Features in Cisco IOS XE 17.9.6 6

Software Features in Cisco IOS XE 17.9.6 6

Whats New in Cisco IOS XE Cupertino 17.9.5 6

Hardware Features in Cisco IOS XE Cupertino 17.9.5 6

Software Features in Cisco IOS XE Cupertino 17.9.5 6

Hardware and Software Behavior Changes in Cisco IOS XE Cupertino 17.9.5 6

Whats New in Cisco IOS XE Cupertino 17.9.4a 6

Whats New in Cisco IOS XE Cupertino 17.9.4 6

Hardware Features in Cisco IOS XE Cupertino 17.9.4 6

Software Features in Cisco IOS XE Cupertino 17.9.4 7

Hardware and Software Behavior Changes in Cisco IOS XE Cupertino 17.9.4 7

Whats New in Cisco IOS XE Cupertino 17.9.3 7

Hardware Features in Cisco IOS XE Cupertino 17.9.3 7
Software Features in Cisco IOS XE Cupertino 17.9.3 7
Hardware and Software Behavior Changes in Cisco IOS XE Cupertino 17.9.3 7
Whats New in Cisco IOS XE Cupertino 17.9.2 7
Hardware Features in Cisco IOS XE Cupertino 17.9.2 7
Software Features in Cisco IOS XE Cupertino 17.9.2 7
Hardware and Software Behavior Changes in Cisco IOS XE Cupertino 17.9.2 7
Whats New in Cisco IOS XE Cupertino 17.9.1 8
Hardware Features in Cisco IOS XE Cupertino 17.9.1 8
Software Features in Cisco IOS XE Cupertino 17.9.1 8
Hardware and Software Behavior Changes in Cisco IOS XE Cupertino 17.9.1 10

CHAPTER 3 **Important Notes** 11
Important Notes 11

CHAPTER 4 **Compatibility Matrix and Web UI System Requirements** 15
Compatibility Matrix 15

CHAPTER 5 **Licensing and Scaling Guidelines** 17
Licensing 17
Available Licensing Models and Configuration Information 17
Scaling Guidelines 17

CHAPTER 6 **Limitations and Restrictions** 19
Limitations and Restrictions 19

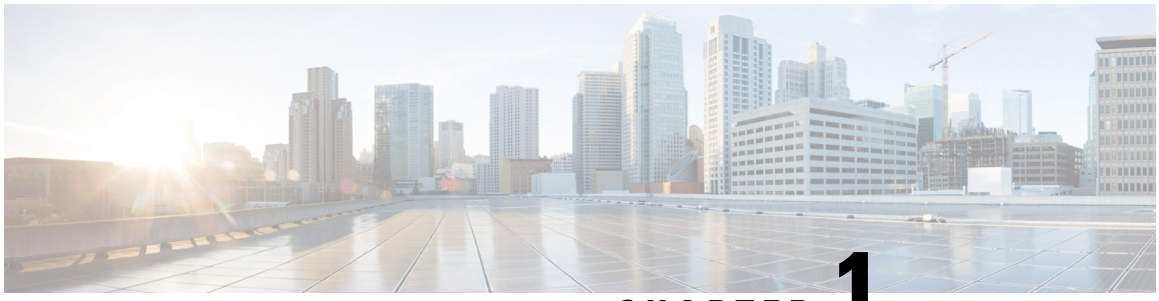
CHAPTER 7 **Boot Loader Versions** 23
Boot Loader Versions 23

CHAPTER 8 **Upgrading the Switch Software** 25
Finding the Software Version 25
Software Images 25
Automatic Boot Loader Upgrade 26

Software Installation Commands 26
Upgrading in Install Mode 27
Downgrading in Install Mode 31

CHAPTER 9 Caveats 37
Cisco Bug Search Tool 37
Open Caveats in Cisco IOS XE Cupertino 17.9.x 37
Resolved Caveats in Cisco IOS XE Cupertino 17.9.9 37
Resolved Caveats in Cisco IOS XE Cupertino 17.9.8 38
Resolved Caveats in Cisco IOS XE Cupertino 17.9.7 38
Resolved Caveats in Cisco IOS XE Cupertino 17.9.6a 38
Resolved Caveats in Cisco IOS XE Cupertino 17.9.6 38
Resolved Caveats in Cisco IOS XE Cupertino 17.9.5 39
Resolved Caveats in Cisco IOS XE Cupertino 17.9.4a 39
Resolved Caveats in Cisco IOS XE Cupertino 17.9.4 39
Resolved Caveats in Cisco IOS XE Cupertino 17.9.3 40
Resolved Caveats in Cisco IOS XE Cupertino 17.9.2 40
Resolved Caveats in Cisco IOS XE Cupertino 17.9.1 40

CHAPTER 10 Additional Information 41
Troubleshooting 41
Related Documentation 41
Communications, Services, and Additional Information 41



CHAPTER 1

Introduction

Cisco Catalyst 9200 Series Switches are entry level enterprise-class access switches that extend the power of intent-based networking and Cisco Catalyst 9000 Series Switches hardware and software innovation to a broader scale of deployments. These switches focus on offering features for the mid-market and simple branchdeployments. With its family pedigree, Cisco Catalyst 9200 Series Switches offer simplicity without compromise - it is secure, always on and provides IT simplicity.

As a foundational building block for Cisco Digital Network Architecture, this platform is built with security, mobility, cloud and IoT at its core. This gives you out of the box upgrades in security, resiliency and programmability regardless of where you are in the intent-based networking journey.

With access to Cisco's best in class security portfolio anchored trustworthy solutions, MACsec encryption and segmentation, the platform provides advanced security features that protect the integrity of the hardware as well as the software and all data that flows through the switch and the network. These switches provide enterprise-level resiliency and keep your business up and running seamlessly with field-replaceable power supplies and fans, modular uplinks, cold patching, perpetual PoE, and the industry's highest mean time between failures (MTBF). Combine the application visibility of full flexible NetFlow with telemetry and the open APIs of Cisco IOS XE and programmability of the UADP ASIC technology and these switches give you the best simple experience provisioning and managing your network now with investment protection on future innovations.

- Supported Hardware, on page 1

Supported Hardware

Cisco Catalyst 9200 Series Switches—Model Numbers

The following table lists the supported hardware models and the default license levels they are delivered with. For information about the available license levels, see section *License Levels*.

Switch Model	Default License Level	Description
C9200-24T-A	Network Advantage	Stackable 24x1G ports; 4x1G and 4x10G fixed uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-24T-E	Network Essentials	

Switch Model	Default License Level	Description
C9200-24P-A	Network Advantage	Stackable 24x1G PoE+ ports; 4x1G and 4x10G fixed uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-24P-E	Network Essentials	
C9200-24PB-A	Network Advantage	Stackable 24x1G PoE+ ports; 4x1G and 4x10G fixed uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-48T-A	Network Advantage	Stackable 48x1G ports; 4x1G and 4x10G fixed uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-48T-E	Network Essentials	
C9200-48P-A	Network Advantage	Stackable 48x1G PoE+ ports; 4x1G and 4x10G fixed uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-48P-E	Network Essentials	
C9200-48PL-A	Network Advantage	Stackable 48x1G PoE+ ports with partial PoE support; 4x1G and 4x10G network modules for uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-48PL-E	Network Essentials	
C9200-48PB-A	Network Advantage	Stackable 48x1G PoE+ ports; 4x1G and 4x10G fixed uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-24PXG-E	Network Essentials	Stackable 8 Multigigabit Ethernet and 16x1G PoE+ ports; supports 4x10G, 2x25G and 2x40G network modules for uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-24PXG-A	Network Advantage	
C9200-48PXG-E	Network Essentials	Stackable 8 Multigigabit Ethernet and 40x1G PoE+ ports; supports 4x10G, 2x25G and 2x40G network modules for uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-48PXG-A	Network Advantage	
C9200L-24P-4G-A	Network Advantage	Stackable 24x1G PoE+ ports; 4x1G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24P-4G-E	Network Essentials	
C9200L-24P-4X-A	Network Advantage	Stackable 24x1G PoE+ ports; 4x10G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24P-4X-E	Network Essentials	
C9200L-24T-4G-A	Network Advantage	Stackable 24x1G ports; 4x1G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24T-4G-E	Network Essentials	
C9200L-24T-4X-A	Network Advantage	Stackable 24x1G ports; 4x10G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24T-4X-E	Network Essentials	

Switch Model	Default License Level	Description
C9200L-48P-4G-A	Network Advantage	Stackable 48x1G PoE+ ports; 4x1G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48P-4G-E	Network Essentials	
C9200L-48P-4X-A	Network Advantage	Stackable 48x1G PoE+ ports; 4x10G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48P-4X-E	Network Essentials	
C9200L-48PL-4G-A	Network Advantage	Stackable 48x1G PoE+ ports with partial PoE support; 4x1G SFP fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48PL-4G-E	Network Essentials	
C9200L-48PL-4X-A	Network Advantage	Stackable 48x1G PoE+ ports with partial PoE support; 4x10G SFP fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48PL-4X-E	Network Essentials	
C9200L-48T-4G-A	Network Advantage	Stackable 48x1G ports; 4x1G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48T-4G-E	Network Essentials	
C9200L-48T-4X-A	Network Advantage	Stackable 48x1G ports; 4x10G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48T-4X-E	Network Essentials	
C9200L-24PXG-4X-A	Network Advantage	Stackable 8xMultigigabit Ethernet PoE+ ports and 16x1G PoE+ ports; 4x10G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24PXG-4X-E	Network Essentials	
C9200L-24PXG-2Y-A	Network Advantage	Stackable 8xMultigigabit Ethernet PoE+ ports and 16x1G PoE+ ports; 2x25G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24PXG-2Y-E	Network Essentials	
C9200L-48PXG-4X-A	Network Advantage	Stackable 12xMultigigabit Ethernet PoE+ ports and 36x1G PoE+ ports; 4x10G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48PXG-4X-E	Network Essentials	
C9200L-48PXG-2Y-A	Network Advantage	Stackable 8xMultigigabit Ethernet PoE+ ports and 40x1G PoE+ ports; 2x25G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48PXG-2Y-E	Network Essentials	
C9200CX-8P-2X2G-A	Network Advantage	8x1G PoE+ ports; 2x1G and 2x10G SFP+ fixed uplink ports; powered using 315W internal power supply unit; fanless.
C9200CX-8P-2X2G-E	Network Essentials	
C9200CX-12P-2X2G-A	Network Advantage	12x1G PoE+ ports; 2x1G and 2x10G SFP+ fixed uplink ports; powered using 315W internal power supply unit; fanless.
C9200CX-12P-2X2G-E	Network Essentials	

Switch Model	Default License Level	Description
C9200CX-12T-2X2G-A	Network Advantage	12x1G Ethernet ports; 2x1G copper uplink ports, 1x1G copper uplink PD port, and 2x10G SFP+ fixed uplink ports; powered either from the copper uplink PD port or using an auxiliary 80W power adapter; fanless
C9200CX-12T-2X2G-E	Network Essentials	

Network Modules

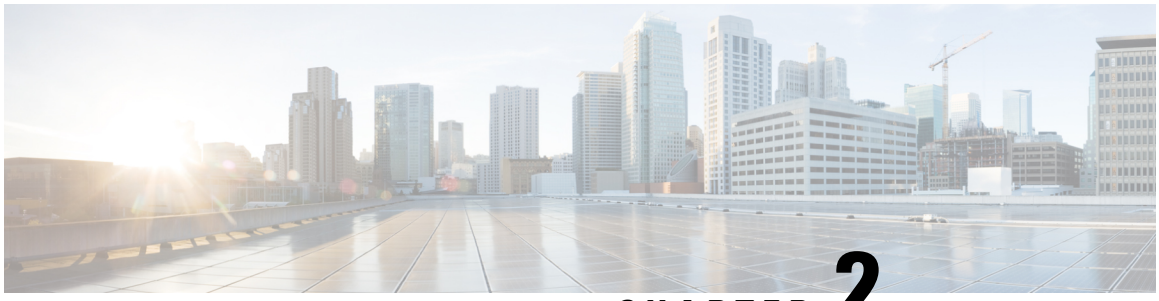
The following table lists the optional uplink network modules with 1-GigabitEthernet and 10-GigabitEthernet slots. You should only operate the switch with either a network module or a blank module installed.

Network Module	Description
C9200-NM-4G [1]	Four 1-GigabitEthernet SFP module slots
C9200-NM-4X [1]	Four 10-GigabitEthernet SFP+ module slots
C9200-NM-2Y[2]	Two 25-GigabitEthernet SFP28 module slots
C9200-NM-2Q[2]	Two 40-GigabitEthernet slots with a QSFP+ connector in each slot

Note These network modules are supported only on the C9200 SKUs of the Cisco Catalyst 9200 Series Switches.

Optics Modules

Cisco Catalyst Series Switches support a wide range of optics and the list of supported optics is updated on a regular basis. Use the Transceiver Module Group (TMG) Compatibility Matrix tool, or consult the tables at this URL for the latest transceiver module compatibility information: https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html



CHAPTER 2

Whats New in Cisco IOS XE Cupertino 17.9.x

- Whats New in Cisco IOS XE Cupertino 17.9.9, on page 5
- Whats New in Cisco IOS XE Cupertino 17.9.8, on page 5
- Whats New in Cisco IOS XE Cupertino 17.9.7, on page 5
- Whats New in Cisco IOS XE Cupertino 17.9.6a, on page 5
- Whats New in Cisco IOS XE Cupertino 17.9.6, on page 6
- Whats New in Cisco IOS XE Cupertino 17.9.5, on page 6
- Whats New in Cisco IOS XE Cupertino 17.9.4a, on page 6
- Whats New in Cisco IOS XE Cupertino 17.9.4, on page 6
- Whats New in Cisco IOS XE Cupertino 17.9.3, on page 7
- Whats New in Cisco IOS XE Cupertino 17.9.2, on page 7
- Whats New in Cisco IOS XE Cupertino 17.9.1, on page 8

Whats New in Cisco IOS XE Cupertino 17.9.9

There are no new features in this release.

Whats New in Cisco IOS XE Cupertino 17.9.8

There are no new features in this release.

Whats New in Cisco IOS XE Cupertino 17.9.7

There are no new features in this release.

Whats New in Cisco IOS XE Cupertino 17.9.6a

There are no new features in this release. This release provides a fix for CSCwm57734: Dot1x auth fail vlan can't assign IP with dhcp.

Whats New in Cisco IOS XE Cupertino 17.9.6

Hardware Features in Cisco IOS XE 17.9.6

There are no new hardware features in this release.

Software Features in Cisco IOS XE 17.9.6

There are no new software features in this release.

Software Features in Cisco IOS XE 17.9.6

There are no new software features in this release.

Whats New in Cisco IOS XE Cupertino 17.9.5

Hardware Features in Cisco IOS XE Cupertino 17.9.5

There are no new hardware features in this release.

Software Features in Cisco IOS XE Cupertino 17.9.5

There are no new software features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Cupertino 17.9.5

There are no behavior changes in Cisco IOS XE Cupertino 17.9.5.

Whats New in Cisco IOS XE Cupertino 17.9.4a

There are no new features in this release. This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

Whats New in Cisco IOS XE Cupertino 17.9.4

Hardware Features in Cisco IOS XE Cupertino 17.9.4

There are no new hardware features in this release.

Software Features in Cisco IOS XE Cupertino 17.9.4

There are no new software features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Cupertino 17.9.4

There are no behavior changes in Cisco IOS XE Cupertino 17.9.4.

Whats New in Cisco IOS XE Cupertino 17.9.3

Hardware Features in Cisco IOS XE Cupertino 17.9.3

There are no new hardware features in this release.

Software Features in Cisco IOS XE Cupertino 17.9.3

There are no new software features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Cupertino 17.9.3

Behavior Change	Description
Inlet Temperature Threshold Values	Yellow and Red thresholds for inlet temperature are modified on Cisco Catalyst 9200CX Series Switches. The new values are: • Yellow Threshold: 74 degree celsius • Red Threshold: 81 degree celsius

Whats New in Cisco IOS XE Cupertino 17.9.2

Hardware Features in Cisco IOS XE Cupertino 17.9.2

There are no new hardware features in this release.

Software Features in Cisco IOS XE Cupertino 17.9.2

There are no new software features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Cupertino 17.9.2

There are no behavior changes in Cisco IOS XE Cupertino 17.9.2.

Whats New in Cisco IOS XE Cupertino 17.9.1

Hardware Features in Cisco IOS XE Cupertino 17.9.1

Feature Name	Description and Documentation Link
Cisco Catalyst 9200 Series Switches (C9200CX)	The following new models have been introduced in the series: • C9200CX-8P-2X2G: 8x1G PoE+ ports; 2x1G and 2x10G SFP+ fixed uplink ports; powered using 310W internal power supply unit; fanless. • C9200CX-12P-2X2G: 12x1G PoE+ ports; 2x1G and 2x10G SFP+ fixed uplink ports; powered using 310W internal power supply unit; fanless. • C9200CX-12T-2X2G: 12x1G Ethernet ports; 3x1G and 2x10G SFP+ fixed uplink ports; the last 1G copper uplink port is a Class 6 PD port capable of powering the switch; also supports 80W auxiliary power adapter; fanless. For more information about the hardware, see the Cisco Catalyst 9200CX Compact Series Switches Hardware Installation Guide.

Software Features in Cisco IOS XE Cupertino 17.9.1

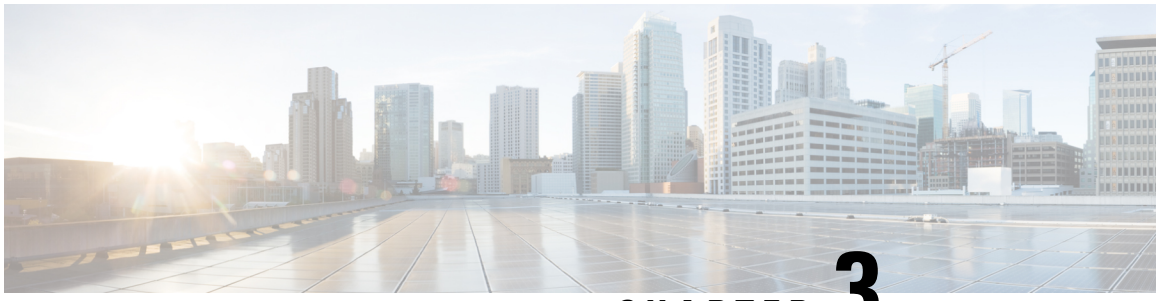
Feature Name	Description
DHCP Snooping with Egress SPAN on the same interface	Introduces support for configuring concurrent DHCP Snooping and egress SPAN on the same interface for non-SDA deployments.
Programmability • YANG Data Models • Pubd Restartability	The following programmability features are introduced in this release: • YANG Data Models: For the list of Cisco IOS XE YANG models available with this release, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1791. Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same GitHub location highlights changes that have been made in the release. (Network Advantage) • Pubd Restartability: The pubd process is restartable on all platforms in this release. Prior to this release, pubd was restartable only on certain platforms. On other platforms, to restart the pubd process, the whole device had to be restarted.

Feature Name	Description
Smart Licensing Using Policy • New mechanism to send data privacy related information • Hostname support	The following Smart Licensing Using Policy features are introduced in this release: • New mechanism to send data privacy related information: This information is no longer included in a RUM report. If data privacy is disabled (**no license smart privacy** { **all** | **hostname** | **version**} global configuration command), data privacy related information is sent in a separate sync message or offline file. Depending on the topology you have implemented, the product instance initiates the sending of this information in a separate message, or CSLU and SSM On-Prem initiates the retrieval of this information from the product instance, or this information is saved in the offline file that is generated when you enter the **license smart save usage** privileged EXEC command. • Hostname support: Support for sending hostname information was introduced. If you configure a hostname on the product instance and disable the corresponding privacy setting (**no license smart privacy hostname** global configuration command), hostname information is sent from the product instance, in a separate sync message or offline file. Depending on the topology you have implemented, the hostname information is received by CSSM, and CSLU or SSM On-Prem. It is then displayed on the corresponding user interface. (Network Advantage)
SMU Installation disabled in bundle mode	Support for SMU installation is disabled in bundle mode. Installation is supported only in install mode. (Network Advantage)
Support for PI SSH	Cisco IOS SSH Server and Client support for the following encryption algorithms have been introduced: • aes128-gcm@openssh.com • aes256-gcm@openssh.com
SXP Version 5	SXP version 5 has been designed to export and import SXP mappings between specified SXP peers. (DNA Advantage)

New on the WebUI
There are no WebUI features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Cupertino 17.9.1

Behavior Change	Description
Custom SDM Templates: Default FIB MAC Address Value	The custom FIB MAC address minimum/default value is 16K. The configurable range for the number of 1k entries is 16 to 128. From Cisco IOS XE Cupertino 17.9.1, this is applicable to *all* subsequent releases.
DHCP Egress Packets Captured in SPAN Sessions	SPAN sessions capture Dynamic Host Configuration Protocol (DHCP) egress packets when DHCP snooping is enabled on the device.
Inlet Temperature Threshold Values	Yellow and Red thresholds for inlet temperature are modified on Cisco Catalyst 9200CX Series Switches. The new values are: • Yellow Threshold: 75 degree celsius • Red Threshold: 85 degree celsius
Last Reload Reason in **show version** command output	The **show version** command output in User EXEC mode is modified. This applies only to stacked switches. Last reload reason does not display error now.
RUM report throttling	For all topologies where the product instance initiates communication, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. The affected topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated communication), *CSLU Disconnected from CSSM* (product instance-initiated communication), and *SSM On-Prem Deployment* (product instance-initiated communication). This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down that was caused by an excessive generation of RUM reports. You can override the reporting frequency throttling, by entering the **license smart sync** command in privileged EXEC mode. This triggers an on-demand synchronization with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases.
show logging onboard switch poe command output	The **show logging onboard switch poe** command output is modified on Cisco Catalyst 9200CX Series Switches. The maximum sensor value is modified.
show vlan mapping command output	The **show vlan mapping** command output is modified. Information about Five GigabitEthernet interface is displayed in the output.



CHAPTER 3

Important Notes

- Important Notes, on page 11

Important Notes

Unsupported Features

- **Cisco TrustSec**
  - Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- **High Availability**
  - Cisco StackWise Virtual
  - Non Stop Forwarding (NSF)
  - Stacking on 9200CX SKUs
- **IP Addressing Services**
  - Gateway Load Balancing Protocol (GLBP)
  - Web Cache Communication Protocol (WCCP)
- **Layer 2**
  - Audio Video Bridging (including IEEE802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav)
- **Multiprotocol Label Switching**
  - Border Gateway Protocol (BGP) on the Cisco Catalyst 9200 Series Switches and Cisco Catalyst 9200L Series Switches
  - Multiprotocol Label Switching (MPLS)
- **Programmability**
  - Programmability (Cisco Plug-in for OpenFlow 1.3, Third-Party Application Hosting)
- **Security**

- IPsec VPN
- MACsec Encryption
  - MACsec configuration on EtherChannel
  - 256-bit AES MACsec (IEEE 802.1AE) host link encryption with MACsec Key Agreement (MKA)
  - MACsec switch-to-host connections in an overlay network.
- Virtual Routing and Forwarding (VRF)-Aware web authentication

- **System Management**
  - Hot patching (for SMUs)
  - Performance Monitoring (PerfMon)

- **VLAN**
  - Private VLAN (PVLAN) on Trunks and Portchannels

- Converged Access for Branch Deployments
- Fabric Enabled Wireless on C9200L SKUs
- Network Load Balancing (NLB)

Complete List of Supported Features

For the complete list of features supported on a platform, see the Cisco Feature Navigator.

Accessing Hidden Commands

This section provides information about hidden commands in Cisco IOS XE and the security measures that are in place, when they are accessed. These commands are only meant to assist Cisco TAC in advanced troubleshooting and are not documented.

Hidden commands are available under:

- Category 1—Hidden commands in privileged or User EXEC mode. Begin by entering the **service internal** command to access these commands.
- Category 2—Hidden commands in one of the configuration modes (global, interface and so on). These commands do not require the **service internal** command.

Further, the following applies to hidden commands under Category 1 and 2:

- The commands have CLI help. Enter enter a question mark (?) at the system prompt to display the list of available commands.

  Note: For Category 1, enter the **service internal** command before you enter the question mark; you do not have to do this for Category 2.

- The system generates a %PARSER-5-HIDDEN syslog message when a hidden command is used. For example:

```
*Feb 14 10:44:37.917: %PARSER-5-HIDDEN: Warning!!! 'show processes memory old-header '
 is a hidden command.
Use of this command is not recommended/supported and will be removed in future.
```

Apart from category 1 and 2, there remain internal commands displayed on the CLI, for which the system does NOT generate the %PARSER-5-HIDDEN syslog message.

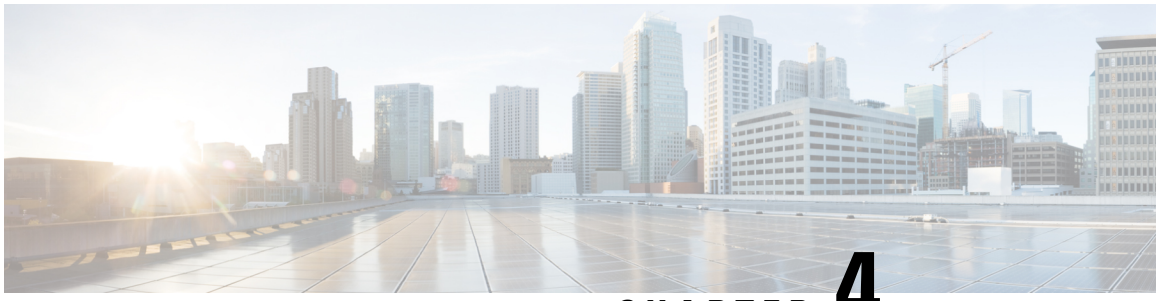
Important We recommend that you use any hidden command only under TAC supervision.

If you find that you are using a hidden command, open a TAC case for help with finding another way of collecting the same information as the hidden command (for a hidden EXEC mode command), or to configure the same functionality (for a hidden configuration mode command) using non-hidden commands.

Default Behaviour

Beginning from Cisco IOS XE Gibraltar 16.12.5 and later, do not fragment bit (DF bit) in the IP packet is always set to 0 for all outgoing RADIUS packets (packets that originate from the device towards the RADIUS server).

Important Notes



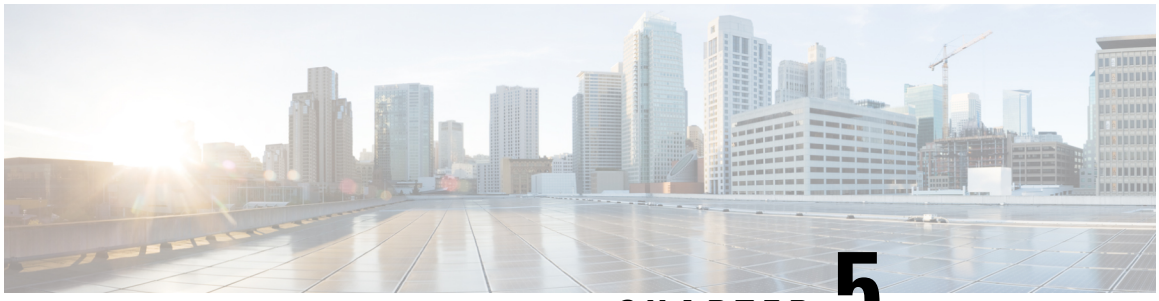
CHAPTER 4

Compatibility Matrix and Web UI System Requirements

- Compatibility Matrix, on page 15

Compatibility Matrix

To view the software compatibility information between Cisco Catalyst 9200 Series Switches, Cisco Identity Services Engine, and Cisco Prime Infrastructure, go to Cisco Catalyst 9000 Series Switches Software Version Compatibility Matrix.



CHAPTER 5

Licensing and Scaling Guidelines

- Licensing, on page 17
- Scaling Guidelines, on page 17

Licensing

For information about licenses required for the features available on Cisco Catalyst 9000 Series Switches, see Configuring Licenses on Cisco Catalyst 9000 Series Switches.

All licensing information relating to Cisco Catalyst 9000 Series Switches are available on this collection page: Cisco Catalyst 9000 Switching Family Licensing.

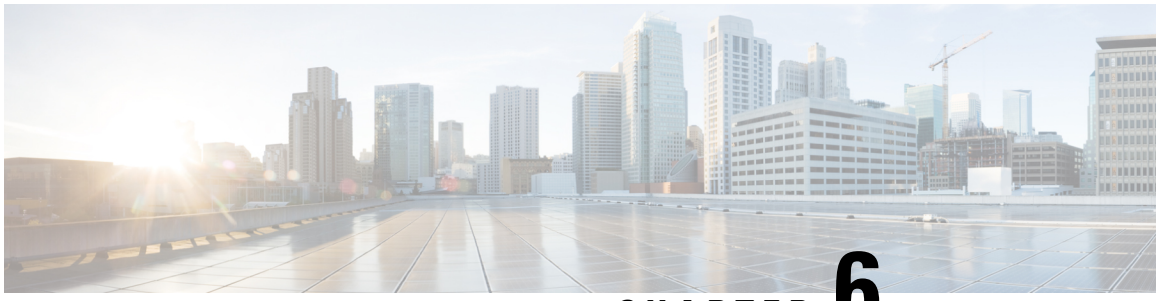
Available Licensing Models and Configuration Information

- Cisco IOS XE Fuji 16.9.2 to Cisco IOS XE Amsterdam 17.3.1: Smart Licensing is the default and the only supported method to manage licenses.
- Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy, which is an enhanced version of Smart Licensing, is the default and the only supported method to manage licenses.

Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst 9200 Series Switches datasheet at:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html



CHAPTER 6

Limitations and Restrictions

• Limitations and Restrictions, on page 19

Limitations and Restrictions

- Control Plane Policing (CoPP)—The **show run** command does not display information about classes configured under `system-cpp policy`, when they are left at default values. Use the **show policy-map system-cpp-policy** or the **show policy-map control-plane** commands in privileged EXEC mode instead.
- Hardware Limitations
  - Management Port—You cannot modify the configured port speed, duplex mode and flow control and disable auto-negotiation on the Ethernet Management port (GigabitEthernet0/0). Port speed and duplex mode can only be changed from a peer port.
  - Network Module — When the C9200-NM-4X network module is plugged into the C9200 SKUs of the Cisco Catalyst 9200 Series Switches, the uplink interface remains in down state until the network module is recognized by the switch. The time taken for the switch to recognize the network module is longer in comparison to the time taken by the switch to recognize other interconnected devices.
  - If the 1-meter and 1.5-meter 10-GBase-CX1 cables, which are connected on the 10-G ports of the Catalyst 9200L switches, are connected to the 10-G peer ports of the Catalyst 9200L or Catalyst 9200 switches, the peer device might go into the error-disabled state because of link flapping if the local device is restarted. As a workaround, run the **shut** and **no shut** commands on the error-disabled peer interfaces.
  - Some DWDM 10G SFPs may take slightly longer (up to 2 seconds) to link up on some variants of the Catalyst 9200 Series Switches. Before the link is up, you may expect to see SymbolErr frames in the output of the **show controller ethernet** command. Once the link is up, SymbolErr frames count stops increasing.
- QoS restrictions
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - Policing and marking policy on sub interfaces is supported.
  - Marking policy on witched virtual interfaces (SVI) is supported.

- QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.

- Secure Shell (SSH)
  - Use SSH Version 2. SSH Version 1 is not supported.
  - When the device is running SCP and SSH cryptographic operations, expect high CPU until the SCP read process is completed. SCP supports file transfers between hosts on a network and uses SSH for the transfer.

    Since SCP and SSH operations are currently not supported on the hardware crypto engine, running encryption and decryption process in software causes high CPU. The SCP and SSH processes can show as much as 40 or 50 percent CPU usage, but they do not cause the device to shutdown.

- Smart Licensing Using Policy: Starting with Cisco IOS XE Amsterdam 17.3.2a, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

  The licensing utilities and user interfaces that are affected by this limitation include only the following: Cisco Smart Software Manager (CSSM), Cisco Smart License Utility (CSLU), and Smart Software Manager On-Prem (SSM On-Prem).

  This limitation is removed from Cisco IOS XE Cupertino 17.9.1. If you configure a hostname and disable hostname privacy (**no license smart privacy hostname** global configuration command), hostname information is sent from the product instance and displayed on the applicable user interfaces (CSSM, CSLU, SSM On-Prem). For more information, see the command reference for this release.

- Stacking
  - Stacking is supported on Cisco Catalyst 9200 Series Switches. A switch stack supports up to eight stack members. However, you cannot stack C9200 SKUs with C9200L SKUs

    The supported stacking bandwidth on C9200L SKUs is up to 80Gbps; on C9200 SKUs, this is up to 160Gbps.
  - The C9200-24PB and C9200-48PB switch models can be stacked only with each other and not with other models of the Cisco Catalyst 9200 Series Switches.
  - Auto upgrade for a new member switch is supported only in the install mode.

- TACACS legacy command: Do not configure the legacy **tacacs-server host** command; this command is deprecated. If the software version running on your device is Cisco IOS XE Gibraltar 16.12.2 or a later release, using the legacy command can cause authentication failures. Use the **tacacs server** command in global configuration mode.

- USB Authentication—When you connect a Cisco USB drive to the switch, the switch tries to authenticate the drive against an existing encrypted preshared key. Since the USB drive does not send a key for authentication, the following message is displayed on the console when you enter **password encryption aes** command:

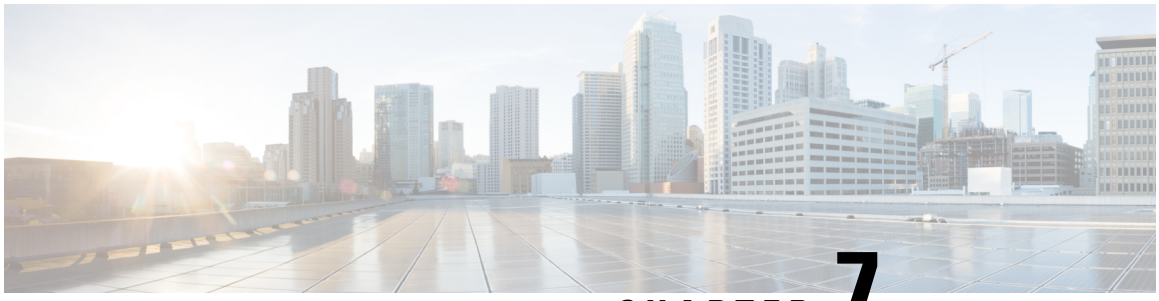
```
Device(config)# password encryption aes
Master key change notification called without new or old key
```

- MACsec is not supported on Software-Defined Access deployments.

- VLAN Restriction—It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.
- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.
- Embedded Event Manager—Identity event detector is not supported on Embedded Event Manager.
- Upgrading the software image from Cisco IOS XE Gibraltar 16.12.x to any of the later releases can result in a persistent database operation failure and after which the persistent database cannot be restored.

  To avoid the persistent database operation failure, use the **dir bootflash:.dbpersist** command to list all DB persist files and then use **delete bootflash:/.dbpersist/folder_name/file_name** and **bootflash:/.dbpersist/folder_name/file_name.meta** commands to delete individual database and meta files from each persistent database folder.
- The File System Check (fsck) utility is not supported in install mode.
- The DiagMemoryTest GOLD test is not supported on the Catalyst 9200 Series Switches.
- On Cisco Catalyst 9200CX Series Switches, zero touch provisioning and guest shell are supported but connecting to an external network from a guest shell does not work, as Management, AppGigabitEthernet, and VirtualPortGroup interfaces are not supported.
- Switch Web UI allows configuration of data VLANs only and not voice VLANs. If you remove a voice VLAN configured to an interface using the Web UI, then all data VLANs associated with the interface are also removed by default.

Limitations and Restrictions



CHAPTER 7

Boot Loader Versions

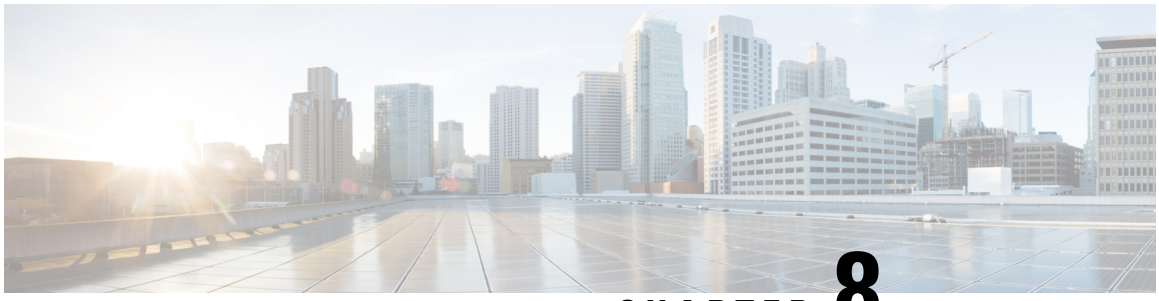
- Boot Loader Versions, on page 23

Boot Loader Versions

The following table provides boot loader version information for the Cisco Catalyst 9200 Series Switches.

Release	ROMMON Version
Cupertino 17.9.9	17.9.1r [FC13]
Cupertino 17.9.8	17.9.1r [FC13]
Cupertino 17.9.7	17.9.1r [FC13]
Cupertino 17.9.6a	17.9.1r [FC13]
Cupertino 17.9.6	17.9.1r [FC13]
Cupertino 17.9.5	17.9.1r [FC13]
Cupertino 17.9.4	17.9.1r [FC13]
Cupertino 17.9.3	17.9.1r [FC11]
Cupertino 17.9.2	17.9.1r [FC8]
Cupertino 17.9.1	17.9.1r [FC8]
Cupertino 17.8.1	17.8.1r [FC5]
Cupertino 17.7.1	17.6.1r [FC1]
Bengaluru 17.6.8	17.9.1r [FC8]
Bengaluru 17.6.7	17.9.1r [FC8]
Bengaluru 17.6.6a	17.9.1r [FC8]
Bengaluru 17.6.6	17.9.1r [FC8]

Release	ROMMON Version
Bengaluru 17.6.5	17.9.1r [FC8]
Bengaluru 17.6.4	17.9.1r [FC8]
Bengaluru 17.6.3	17.8.1r [FC5]
Bengaluru 17.6.2	17.6.1r [FC1]
Bengaluru 17.6.1	17.6.1r [FC1]
Bengaluru 17.5.1	17.5.1r [FC4]
Bengaluru 17.4.1	17.4.1r [FC3]
Amsterdam 17.3.8a	17.9.1r [FC8]
Amsterdam 17.3.8	17.9.1r [FC8]
Amsterdam 17.3.7	17.9.1r [FC8]
Amsterdam 17.3.6	17.9.1r [FC8]
Amsterdam 17.3.5	17.5.1r [FC4]
Amsterdam 17.3.4	17.5.1r [FC4]
Amsterdam 17.3.3	17.5.1r [FC4]
Amsterdam 17.3.2a	17.3.1r [FC4]
Amsterdam 17.3.1	17.3.1r [FC3]
Amsterdam 17.2.1	17.2.1r [FC2]
Amsterdam 17.1.1	17.1.1 [FC3]



CHAPTER 8

Upgrading the Switch Software

- Finding the Software Version, on page 25
- Software Images, on page 25
- Automatic Boot Loader Upgrade, on page 26
- Software Installation Commands, on page 26
- Upgrading in Install Mode, on page 27
- Downgrading in Install Mode, on page 31

Finding the Software Version

The package files for the Cisco IOS XE software are stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch.

Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the **dir** *filesystem:* privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Software Images

Release	Image Type	File Name
Cisco IOS XE Cupertino 17.9.9	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.09.09.SPA.bin
Cisco IOS XE Cupertino 17.9.8	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.09.08.SPA.bin
Cisco IOS XE Cupertino 17.9.7	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.09.07.SPA.bin
Cisco IOS XE Cupertino 17.9.6a	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.09.06a.SPA.bin

Release	Image Type	File Name
Cisco IOS XE Cupertino 17.9.6	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.09.06.SPA.bin
Cisco IOS XE Cupertino 17.9.5	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.09.05.SPA.bin
Cisco IOS XE Cupertino 17.9.4a	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.09.04a.SPA.bin
Cisco IOS XE Cupertino 17.9.4	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.09.04.SPA.bin
Cisco IOS XE Cupertino 17.9.3	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.09.03.SPA.bin
Cisco IOS XE Cupertino 17.9.2	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.09.02.SPA.bin
Cisco IOS XE Cupertino 17.9.1	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.09.01.SPA.bin

Automatic Boot Loader Upgrade

When you upgrade from the existing release on your switch to a later or newer release for the first time, the boot loader may be automatically upgraded, based on the hardware version of the switch. If the boot loader is automatically upgraded, it will take effect on the next reload. If you go back to the older release after this, the boot loader is not downgraded. The updated boot loader supports all previous releases.

Caution Do not power cycle your switch during the upgrade.

Software Installation Commands

Summary of Software Installation Commands	
To install and activate the specified file, and to commit changes to be persistent across reloads: **`install add file`** *`filename`* [**`activate commit`**] To separately install, activate, commit, cancel, or remove the installation file: **`install ?`**	
add file tftp: *filename*	Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.
activate [**auto-abort-timer**]	Activates the file, and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Upgrading in Install Mode

Follow these instructions to upgrade from one release to another, in install mode. To perform a software image upgrade, you must be booted into IOS through **boot flash:packages.conf**.

Before you begin

Note that you can use this procedure for the following upgrade scenarios:

When upgrading from ...	To...
Cisco IOS XE Cupertino 17.8.x or earlier releases	Cisco IOS XE Cupertino 17.9.x

The sample output in this section displays upgrade from Cisco IOS XE Cupertino 17.8.1 to Cisco IOS XE Cupertino 17.9.1 using **install** commands only.

Procedure

Step 1 Clean-up

install remove inactive

Use this command to clean-up old installation files in case of insufficient space and to ensure that you have at least 1GB of space in flash, to expand a new image.

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command:

```
Switch# install remove inactive
install_remove: START Mon Jul 25 17:46:18 IST 2022
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat9k_lite-rpbase.17.08.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.17.08.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.17.08.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.17.08.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

The following files will be deleted:
[switch 1]:
/flash/cat9k_lite_iosxe.17.08.01.SPA.bin

Do you want to remove the above files? [y/n]y

[switch 1]:
Deleting file flash:cat9k_lite_iosxe.17.08.01.SPA.bin ... done.
SUCCESS: Files deleted.
```

```
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
  [1] Post_Remove_Cleanup package(s) on switch 1
  [1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup
SUCCESS: install_remove  Mon Jul 25 17:47:20 IST 2022
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp:***[[//location]/directory]/filename***flash:**

Use this command to copy the new image from a TFTP server to flash memory. The location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers. Skip this step if you want to use the new image from a TFTP server.

```
Switch# copy tftp://10.8.0.6/image/cat9k_lite_iosxe.17.09.01.SPA.bin flash:

Destination filename [cat9k_lite_iosxe.17.09.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_lite_iosxe.17.09.01.SPA.bin...
Loading /cat9k_lite_iosxe.17.09.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!
```

Use this command to verify the boot variable (packages.conf) and manual boot setting (no):

```
Switch# show boot
--------------------------
Switch 3
--------------------------
Current Boot Variables:
BOOT variable = flash:packages.conf;

Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = no
Enable Break = yes
Boot Mode = DEVICE
iPXE Timeout = 0
```

Step 4 Install image to flash

install add file activate commit

Use this command to install the image.

We recommend that you point to the source image on your TFTP server or the flash drive of the switch, if you have copied the image to flash memory.

The following sample output displays installation of the Cisco IOS XE Cupertino 17.9.1 software image in the flash memory:

```
Switch# install add file flash:cat9k_lite_iosxe.17.09.01.SPA.bin activate commit
install_add_activate_commit: START Mon Jul 25 12:51:55 IST 2022
Jul 25 12:51:57.795: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
one-shot flash:cat9k_lite_iosxe.17.09.01.SPA.bin
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_lite_iosxe.17.09.01.SPA.bin to the selected switch(es)
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
  [1] Add package(s) on switch 1
  [1] Finished Add on switch 1
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

Image added. Version: 17.09.01.0.276
install_add_activate_commit: Activating PACKAGE

gzip: initramfs.cpio.gz: decompression OK, trailing garbage ignored
Following packages shall be activated:
/flash/cat9k_lite-webui.17.09.01.SPA.pkg
/flash/cat9k_lite-srdriver.17.09.01.SPA.pkg
/flash/cat9k_lite-rpboot.17.09.01.SPA.pkg
/flash/cat9k_lite-rpbase.17.09.01.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on all members
Jul 25 13:03:24.337: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds
  [1] Activate package(s) on switch 1
```

```
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k_lite-rpbase.17.08.01.SPA.pkg
      Removed cat9k_lite-rpboot.17.08.01.SPA.pkg
      Removed cat9k_lite-srdriver.17.08.01.SPA.pkg
      Removed cat9k_lite-webui.17.08.01.SPA.pkg
    New files list:
      Added cat9k_lite-rpbase.17.09.01.SPA.pkg
      Added cat9k_lite-rpboot.17.09.01.SPA.pkg
      Added cat9k_lite-srdriver.17.09.01.SPA.pkg
      Added cat9k_lite-webui.17.09.01.SPA.pkg
    Finished list of software package changes
  [1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

*Jul 25 13:03:24.298 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds--- Starting Commit ---
Performing Commit on all members
  [1] Commit package(s) on switch 1
  [1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Mon Jul 25 13:04:23 IST 2022
Jul 25 13:04:24.586: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE flash:cat9k_lite_iosxe.17.09.01.SPA.bin
```

Note
The system reloads automatically after executing the **install add file activate commit command**. You do not have to manually reload the system.

Step 5 Verify installation

After the software has been successfully installed, use this command to verify that the flash partition has four new `.pkg` files and two `.conf` files.

a) **dir flash:*.pkg**

The following is sample output of the **dir flash:*.pkg** command:

```
Switch# dir flash:*.pkg

Directory of flash:/*.pkg
Directory of flash:/
48582  -rw- 298787860  Apr 20 2022 05:13:32 +00:00  cat9k_lite-rpbase.17.08.01.SPA.pkg
48585  -rw- 35713901   Apr 20 2022 05:14:12 +00:00  cat9k_lite-rpboot.17.08.01.SPA.pkg
48583  -rw- 4252692    Apr 20 2022 05:13:33 +00:00  cat9k_lite-srdriver.17.08.01.SPA.pkg
48584  -rw- 8119312    Apr 20 2022 05:13:34 +00:00  cat9k_lite-webui.17.08.01.SPA.pkg

16640  -rw- 301188116   Jul 25 2022 05:33:25 +00:00  cat9k_lite-rpbase.17.09.01.SPA.pkg
16647  -rw- 35112025    Jul 25 2022 05:34:06 +00:00  cat9k_lite-rpboot.17.09.01.SPA.pkg
16642  -rw- 4326420    Jul 25 2022 05:33:25 +00:00  cat9k_lite-srdriver.17.09.01.SPA.pkg
16643  -rw- 8328208     Jul 25 2022 05:33:25 +00:00  cat9k_lite-webui.17.09.01.SPA.pkg
```

b) **dir flash:*.conf**

The following is sample output of the **dir flash:*.conf** command. It displays the .conf files in the flash partition; note the two .conf files:

- `packages.conf`—the file that has been re-written with the newly installed .pkg files
- `cat9k_lite_iosxe.17.09.01.SPA.conf`— a backup copy of the newly installed packages.conf file

```
Switch# dir flash:*.conf

Directory of flash:/*.conf
Directory of flash:/

16631 -rw- 4882  Jul 25 2022 05:39:42 +00:00  packages.conf
16634 -rw- 4882  Jul 25 2022 05:34:06 +00:00  cat9k_lite_iosxe.17.09.01.SPA.conf
```

Step 6 Reload and verify version

a) **reload**

Use this command to reload the switch. When you boot the new image, the boot loader is automatically updated, but the new bootloader version is not displayed in the output until the next reload.

```
Switch# reload
```

b) **show version**

After the image boots up, use this command to verify the version of the new image.

The following sample output of the **show version** command displays the Cisco IOS XE Cupertino 17.9.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.09.01
Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version
 17.9.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Mon 4-Apr-21 19:57 by mcpre
<output truncated>
```

Downgrading in Install Mode

Follow these instructions to downgrade from one release to another, in install mode. To perform a software image downgrade, you must be booted into IOS through **boot flash:packages.conf**.

Before you begin

Note that you can use this procedure for the following downgrade scenarios:

When downgrading from ...	To ...
Cisco IOS XE Cupertino 17.9.x	Cisco IOS XE Cupertino 17.8.x or earlier releases.

Note New switch models that are introduced in a release cannot be downgraded. The release in which a switch model is introduced is the minimum software version for that model.

The sample output in this section shows downgrade from Cisco IOS XE Cupertino 17.9.1 to Cisco IOS XE Cupertino 17.8.1, using **install** commands.

Procedure

Step 1 Clean-up

install remove inactive

Use this command to clean-up old installation files in case of insufficient space and to ensure that you have at least 1GB of space in flash, to expand a new image.

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command:

```
Switch# install remove inactive
install_remove: START Mon Jul 25 17:46:18 IST 2022
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat9k_lite-rpbase.17.09.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.17.09.1.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.17.09.1.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.17.09.1.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

The following files will be deleted:
[switch 1]:
/flash/cat9k_lite_iosxe.17.09.1.SPA.bin

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k_lite_iosxe.17.09.1.SPA.bin ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
  [1] Post_Remove_Cleanup package(s) on switch 1
  [1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup

SUCCESS: install_remove  Mon Jul 25 17:47:20 IST 2022
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp:***[[//location]/directory]/filename***flash:**

Use this command to copy the new image from a TFTP server to flash memory. The location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers. Skip this step if you want to use the new image from a TFTP server.

```
Switch# copy tftp://10.8.0.6/image/cat9k_lite_iosxe.17.08.1.SPA.bin flash:

Destination filename [cat9k_lite_iosxe.17.08.1.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_lite_iosxe.17.08.1.SPA.bin...
Loading /cat9k_lite_iosxe.17.08.1.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!
```

Use this command to install the image.

We recommend that you point to the source image on your TFTP server or the flash drive of the switch, if you have copied the image to flash memory.

The following example displays the installation of the Cisco IOS XE Cupertino 17.8.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_lite_iosxe.17.08.01.SPA.bin activate commit

install_add_activate_commit: START Mon Jul 25 13:17:28 IST 2022
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_lite_iosxe.17.08.01.SPA.bin to the selected switch(es)
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
  [1] Add package(s) on switch 1
  [1] Finished Add on switch 1
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

Image added. Version: 17.08.01.0.203
install_add_activate_commit: Activating PACKAGE

gzip: initramfs.cpio.gz: decompression OK, trailing garbage ignored
Following packages shall be activated:
/flash/cat9k_lite-webui.17.08.01.SPA.pkg
/flash/cat9k_lite-srdriver.17.08.01.SPA.pkg
/flash/cat9k_lite-rpboot.17.08.01.SPA.pkg
/flash/cat9k_lite-rpbase.17.08.01.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on all members
Jul 25 13:29:31.133: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds

*Jul 25 13:29:31.093 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds  [1] Activate package(s)
 on switch 1
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k_lite-rpbase.17.09.01.SPA.pkg
      Removed cat9k_lite-rpboot.17.09.01.SPA.pkg
      Removed cat9k_lite-srdriver.17.09.01.SPA.pkg
      Removed cat9k_lite-webui.17.09.01.SPA.pkg
    New files list:
      Added cat9k_lite-rpbase.17.08.01.SPA.pkg
      Added cat9k_lite-rpboot.17.08.01.SPA.pkg
      Added cat9k_lite-srdriver.17.08.01.SPA.pkg
      Added cat9k_lite-webui.17.08.01.SPA.pkg
    Finished list of software package changes
  [1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
```

```
  [1] Commit package(s) on switch 1
  [1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Send model notification for install_add_activate_commit before reload
Install will reload the system now!
SUCCESS: install_add_activate_commit  Mon Jul 25 13:30:52 IST 2022
Jul 25 13:30:53.573: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE flash:cat9k_lite_iosxe.17.08.01.SPA.bin
Jul 25 13:30:53.573 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE flash:cat9k_lite_iosxe.17.08.01.SPA.bin

switch3#
Chassis 1 reloading, reason - Reload command

*Jul 25 13:30:53.529 IST: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_engine:
 Completed install one-shot PACKAGE flash:cat9k_lite_iosxe.17.08.01.SPA.bin
*Jul 25 13:30:54.526 IST: %STACKMGR-1-RELOAD: Switch 1 R0/0: stack_mgr: Reloading due to
reason Reload command Jul 25 13:30:58.121: %PMAN-5-EXITACTION: F0/0: pvp: Process manager
is exiting: reload fp actionrequested
Jul 25 13:31:01.303: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes
 exit with reload switch code
```

Note
The system reloads automatically after executing the **install add file activate commit** command. You do not have to manually reload the system.

Step 5 Verify version

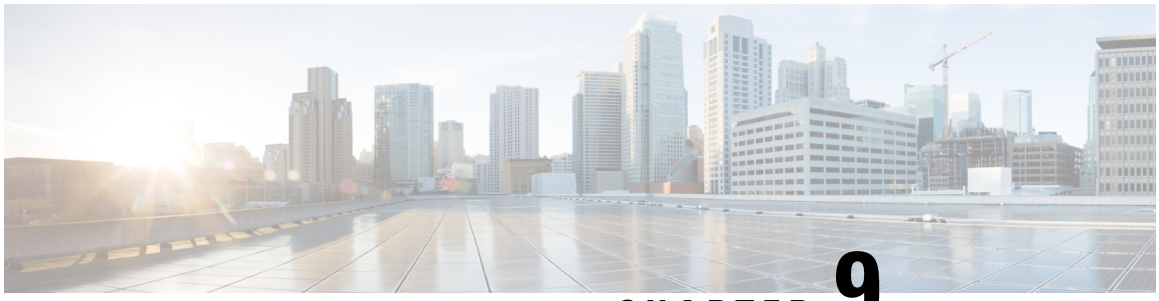
show version

After the image boots up, use this command to verify the version of the new image.

Note
When you downgrade the software image, the bootloader version does not downgrade. It remains updated.

The following sample output of the **show version** command displays the Cisco IOS XE Cupertino 17.8.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.08.01
Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version
17.8.1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
<output truncated>
```



CHAPTER 9

Caveats

- Cisco Bug Search Tool, on page 37
- Open Caveats in Cisco IOS XE Cupertino 17.9.x, on page 37
- Resolved Caveats in Cisco IOS XE Cupertino 17.9.9, on page 37
- Resolved Caveats in Cisco IOS XE Cupertino 17.9.8, on page 38
- Resolved Caveats in Cisco IOS XE Cupertino 17.9.7, on page 38
- Resolved Caveats in Cisco IOS XE Cupertino 17.9.6a, on page 38
- Resolved Caveats in Cisco IOS XE Cupertino 17.9.6, on page 38
- Resolved Caveats in Cisco IOS XE Cupertino 17.9.5, on page 39
- Resolved Caveats in Cisco IOS XE Cupertino 17.9.4a, on page 39
- Resolved Caveats in Cisco IOS XE Cupertino 17.9.4, on page 39
- Resolved Caveats in Cisco IOS XE Cupertino 17.9.3, on page 40
- Resolved Caveats in Cisco IOS XE Cupertino 17.9.2, on page 40
- Resolved Caveats in Cisco IOS XE Cupertino 17.9.1, on page 40

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat, click on the identifier.

Open Caveats in Cisco IOS XE Cupertino 17.9.x

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Cupertino 17.9.9

Identifier	Headline
CSCwo40128	ISR1000 could experience an unexpected reload while connecting with MFA

Identifier	Headline
CSCwq01495	Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability

Resolved Caveats in Cisco IOS XE Cupertino 17.9.8

There are no resolved caveats in this release

Resolved Caveats in Cisco IOS XE Cupertino 17.9.7

There are no resolved caveats in this release

Resolved Caveats in Cisco IOS XE Cupertino 17.9.6a

Identifier	Headline
CSCwm57734	Dot1x auth fail vlan can't assign IP with dhcp

Resolved Caveats in Cisco IOS XE Cupertino 17.9.6

Identifier	Headline
CSCwk15432	Faulty PWR-C6-600WAC blocks PSU slot to recognize known wokring good PSU
CSCwi62480	'show inventory ' shows 'Unknown uplink module' for FRU uplink module when reload Cat9200
CSCwk82261	Switch dropping TCP SYN packets <Random Port> DOT1X, MAB configuration.
CSCwj21346	C9200 Half-ring Stack, but the "Link OK" and "Sync OK" indicators show "yes"
CSCwk27064	%SFF8472-3-READ_ERROR: Gi2/1/1: Error reading DOM data from transceiver
CSCwi32052	Endpoints lose network connection when macsec is enabled.
CSCwj03295	GigabitEthernet ports connected to other Catalyst device go down when Switchover
CSCwk80732	Some of oid does not show output of MGMT port
CSCwi60084	Cat9200L may experience an Unexpected Reload
CSCwk62333	Cat9200L Unexpected reload crimson db write lock held for too long
CSCwk84047	Memory Leak due to security violation by new MAC address and "'Del Pend" object increases - ACE_IPV4

Identifier	Headline
CSCwk50488	Memory leak in fman_rp under acl_db

Resolved Caveats in Cisco IOS XE Cupertino 17.9.5

Identifier	Headline
CSCwi30269	Port 2228 isn't closed after reload when l2-traceroute is disabled, Security threat
CSCwf68913	C9000: Interface link flapping(down/up) occurs at active switch after switchover
CSCwh29961	Show stacks: Information of Last System Crash:%Error opening crashinfo:crashinfo_RP_00_00
CSCwe65441	Non-PoE 9200/9200L devices with ARTXXX power supply present in Slot A do not boot after switch power cycle
CSCwf18420	LLDP does not announce dynamically assigned VLAN
CSCwf23122	Catalyst 9200 might reload due to REPM process crash
CSCwe95691	PnP | Cat9k sends DHCP Discover with IP Source address 192.168.1.1 instead of 0.0.0.0
CSCwi10405	[NEAT] CISP installs a static MAC address entry pointing to a wrong interface

Resolved Caveats in Cisco IOS XE Cupertino 17.9.4a

Identifier	Headline
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

Resolved Caveats in Cisco IOS XE Cupertino 17.9.4

Identifier	Headline
CSCwe33886	17.9 install oper DB queries returning errors on DB queries to xpath install-oper-hist
CSCwe36743	Segmentation Fault - Crash - SSH - When Changing AAA Group Configs
CSCwe73012	9130/9166 APs are not powering up when connected to Gig port of C9200-CX switch
CSCwe79786	C9200CX: entSensorThresholdValue shows wrong yellow threshold
CSCwe91069	C9200 Unexpected reload upon removing netflow commands

Identifier	Headline
CSCwe89814	Unexpected reboot due to FED process heldown with Netflow
CSCwc41288	C9200L - Input Errors on Uplinks using 1G SFP
CSCwe79864	C9200: Incorrect Iout, pout and PS fan rpm speeds in "show env all" CLI

Resolved Caveats in Cisco IOS XE Cupertino 17.9.3

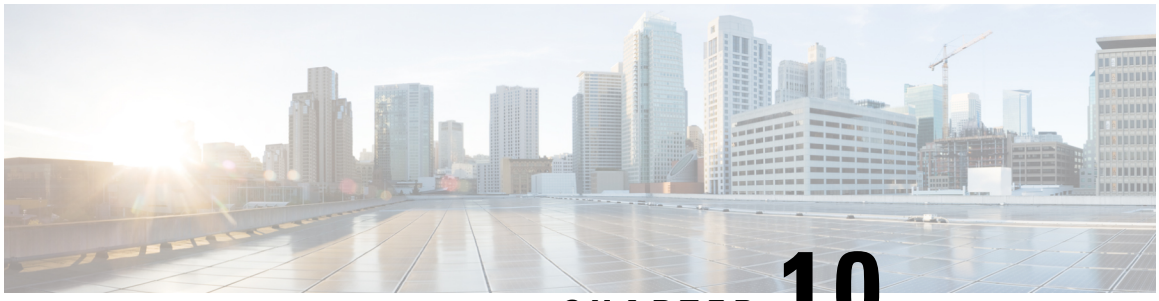
Identifier	Headline
CSCwd56540	Ignore higher fan speed deviations on 9200

Resolved Caveats in Cisco IOS XE Cupertino 17.9.2

Identifier	Headline
CSCwc84941	Due to signal suppression enabled the map-requests are not sent when below map-cache limit

Resolved Caveats in Cisco IOS XE Cupertino 17.9.1

Identifier	Headline
CSCvz77502	9200l 10G port led not blinking green under speed mode
CSCwa23654	Memory leak in Inline Power IOSd process when PoE is used
CSCwa41298	remote switch doesn't detect link down when one rx fiber cable is unplugged on 9200L
CSCwa52014	CISCO-ENHANCED-MEMPOOL-MIB not working on C9200 and C9300
CSCwa76242	Cat 9200L - 10G Link Flaps at intermittent times when peer is maintained as Nexus 9K
CSCwa77415	Switch stack shows wrong neighbor info for stack-ports links
CSCwb18702	CISCO-ENTITY-SENSOR-MIB is returning wrong threshold values for thermal sensors
CSCwb76541	IOSd Crashes in "Call Home cert update" Process During Trustpool Download



CHAPTER 10

Additional Information

- Troubleshooting, on page 41
- Related Documentation, on page 41
- Communications, Services, and Additional Information, on page 41

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:

https://www.cisco.com/en/US/support/index.html

Go to **Product Support** and select your product from the list or enter the name of your product. Look under Troubleshoot and Alerts, to find information for the problem that you are experiencing.

Related Documentation

Information about Cisco IOS XE at this URL: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html

All support documentation for Cisco Catalyst 9200 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9200-r-series-switches/tsd-products-support-series-home.html

Cisco Validated Designs documents at this URL: https://www.cisco.com/go/designzone

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: https://cfnng.cisco.com/mibs

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.

- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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

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

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

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

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

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

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

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

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)

© 2025 Cisco Systems, Inc. All rights reserved.