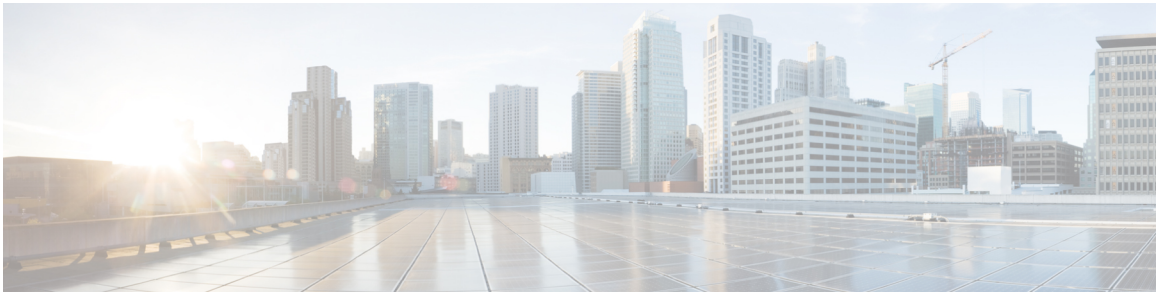


Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS XE Dublin 17.12.x

First Published: 2023-07-28

Last Modified: 2026-03-27

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

What's New in Cisco IOS XE Dublin 17.12.x 5

Hardware Features in Cisco IOS XE 17.12.7a 5

Software Features in Cisco IOS XE 17.12.7a 5

Hardware and Software Behavior Changes in CIsco IOS XE Dublin 17.12.7a 6

Hardware Features in Cisco IOS XE 17.12.6 6

Software Features in Cisco IOS XE 17.12.6 6

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.6 6

Hardware Features in Cisco IOS XE 17.12.5 6

Software Features in Cisco IOS XE 17.12.5 6

Hardware and Software Behavior Changes in CIsco IOS XE Dublin 17.12.5 6

Hardware Features in Cisco IOS XE Dublin 17.12.4 6

Software Features in Cisco IOS XE Dublin 17.12.4 7

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.4 7

Hardware Features in Cisco IOS XE Dublin 17.12.3 7

Software Features in Cisco IOS XE Dublin 17.12.3 7

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.3 7

Hardware Features in Cisco IOS XE Dublin 17.12.2 7

Software Features in Cisco IOS XE Dublin 17.12.2 7

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.2 7

Hardware Features in Cisco IOS XE Dublin 17.12.1 8
Software Features in Cisco IOS XE Dublin 17.12.1 8
Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.1 10

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

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

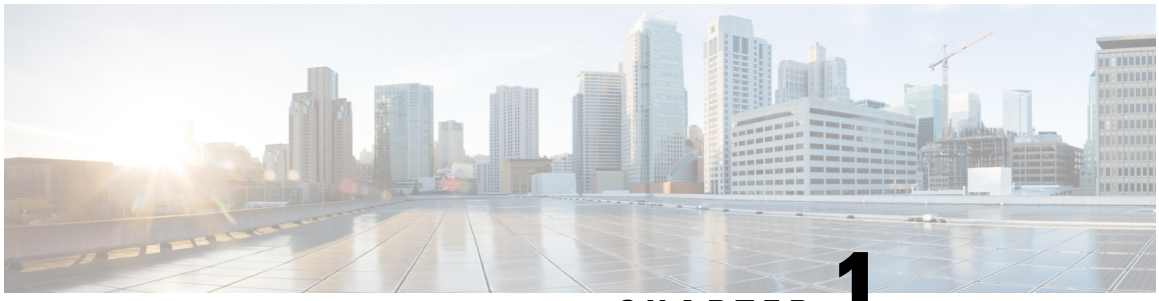
CHAPTER 8 **Upgrading the Switch Software** 25
Finding the Software Version 25
Software Images 25
Automatic Boot Loader Upgrade 26
Software Installation Commands 26
Upgrading in Install Mode 27
Downgrading in Install Mode 31

CHAPTER 9 **Caveats** 37
Cisco Bug Search Tool 37
Open Caveats in Cisco IOS XE Dublin 17.12.x 37

Resolved Caveats in Cisco IOS XE Dublin 17.12.7a 38
Resolved Caveats in Cisco IOS XE Dublin 17.12.6 38
Resolved Caveats in Cisco IOS XE Dublin 17.12.5 38
Resolved Caveats in Cisco IOS XE Dublin 17.12.4 38
Resolved Caveats in Cisco IOS XE Dublin 17.12.3 39
Resolved Caveats in Cisco IOS XE Dublin 17.12.2 39
Resolved Caveats in Cisco IOS XE Dublin 17.12.1 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	
C9200CX-12P-2XGH-A	Network Advantage	12x1G PoE+ ports; 2x10G SFP+ and 2x1G Copper fixed uplink ports; powered using 315W HVDC/AC internal power supply unit; fanless.
C9200CX-12P-2XGH-E	Network Essentials	
C9200CX-8P-2XGH-A	Network Advantage	8x1G PoE+ ports; 2x10G SFP+ and 2x1G Copper fixed uplink ports; powered using 315W HVDC/AC internal power supply unit; fanless.
C9200CX-8P-2XGH-E	Network Essentials	
C9200CX-8UXG-2X-A	Network Advantage	8 ports UPOE (with 4x1G and 4xmGig ports with speed up to 10G), 2x 10G SFP+ fixed uplinks, powered using 315W internal power supply unit; fanless
C9200CX-8UXG-2X-E	Network Essentials	
C9200CX-8UXG-2XH-A	Network Advantage	8 ports UPOE (with 4x1G and 4xmGig ports with speed up to 10G), 2x 10G SFP+ fixed uplinks, powered using 315W HVDC/AC internal power supply unit; fanless.
C9200CX-8UXG-2XH-E	Network Essentials	

Network Modules

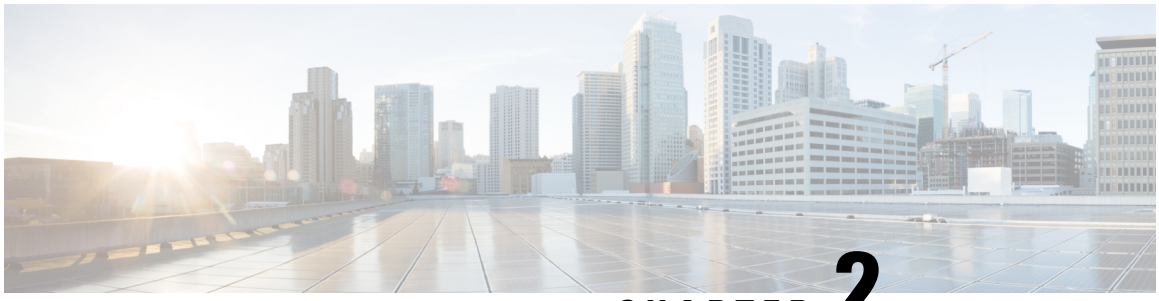
The following table lists the optional uplink network modules with 1-GigabitEthernet and 10-GigabitEthernet slots. You should only operate the switch with either a network module or a blank module installed.

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

What's New in Cisco IOS XE Dublin 17.12.x

- Hardware Features in Cisco IOS XE 17.12.7a, on page 5
- Software Features in Cisco IOS XE 17.12.7a, on page 5
- Hardware and Software Behavior Changes in CIsco IOS XE Dublin 17.12.7a, on page 6
- Hardware Features in Cisco IOS XE 17.12.6, on page 6
- Software Features in Cisco IOS XE 17.12.6, on page 6
- Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.6, on page 6
- Hardware Features in Cisco IOS XE 17.12.5, on page 6
- Software Features in Cisco IOS XE 17.12.5, on page 6
- Hardware and Software Behavior Changes in CIsco IOS XE Dublin 17.12.5, on page 6
- Hardware Features in Cisco IOS XE Dublin 17.12.4, on page 6
- Software Features in Cisco IOS XE Dublin 17.12.4, on page 7
- Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.4, on page 7
- Hardware Features in Cisco IOS XE Dublin 17.12.3, on page 7
- Software Features in Cisco IOS XE Dublin 17.12.3, on page 7
- Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.3, on page 7
- Hardware Features in Cisco IOS XE Dublin 17.12.2, on page 7
- Software Features in Cisco IOS XE Dublin 17.12.2, on page 7
- Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.2, on page 7
- Hardware Features in Cisco IOS XE Dublin 17.12.1, on page 8
- Software Features in Cisco IOS XE Dublin 17.12.1, on page 8
- Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.1, on page 10

Hardware Features in Cisco IOS XE 17.12.7a

There are no new hardware features in this release.

Software Features in Cisco IOS XE 17.12.7a

There are no new software features in this release.

Hardware and Software Behavior Changes in CIsco IOS XE Dublin 17.12.7a

There are no behavior changes in this release.

Hardware Features in Cisco IOS XE 17.12.6

There are no new hardware features in this release.

Software Features in Cisco IOS XE 17.12.6

There are no new software features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.6

There are no behavior changes in this release.

Hardware Features in Cisco IOS XE 17.12.5

There are no new hardware features in this release.

Software Features in Cisco IOS XE 17.12.5

There are no new software features in this release.

Hardware and Software Behavior Changes in CIsco IOS XE Dublin 17.12.5

There are no behavior changes in this release.

Hardware Features in Cisco IOS XE Dublin 17.12.4

There are no new hardware features in this release.

Software Features in Cisco IOS XE Dublin 17.12.4

There are no new software features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.4

There are no behavior changes in this release.

Hardware Features in Cisco IOS XE Dublin 17.12.3

There are no new hardware features in this release.

Software Features in Cisco IOS XE Dublin 17.12.3

There are no new software features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.3

There are no behavior changes in this release.

Hardware Features in Cisco IOS XE Dublin 17.12.2

There are no new hardware features in this release.

Software Features in Cisco IOS XE Dublin 17.12.2

There are no new software features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.2

There are no behavior changes in this release.

Hardware Features in Cisco IOS XE Dublin 17.12.1

There are no new hardware features in this release.

Software Features in Cisco IOS XE Dublin 17.12.1

Feature Name	Description
DSCP marking for RADIUS packets for administrative sessions	Allows you to configure DSCP marking for RADIUS packets for administrative sessions such as SSH and Telnet. (Network Essentials)
Interface ID Option in DHCPv6 Relay Message	Introduces support for interface ID option in DHCPv6 Relay message. With this, the physical interface details of the client interface are included along with the VLAN number in the message. (Network Essentials and Network Advantage)
Interface Template Support for IPv6 DHCP Guard	Enables you to add the **ipv6 dhcp guard attach-policy** *policy_name* global configuration command to an interface template. IPv6 DHCP Guard is then enabled and the policy is applied, wherever the template is applied. (Network Advantage)
IP DHCP Server Changes to Limit IP Assignment to Next Hop only	Allows you to assign DHCP IP address only to the neighbouring device in an interface using the **ip dhcp restrict next hop** command. When this command is enabled, the DHCP server in the interface uses the MAC addresses in the DHCP packet and compares it with the addresses in the Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) cache table. If the MAC addresses match, then the DHCP IP address is assigned to that device. (Network Advantage)

Feature Name	Description

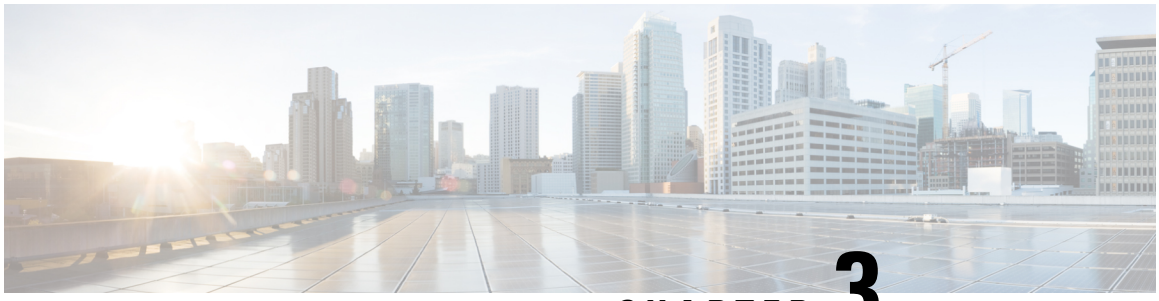
Modified Trustpoints for Secure Unique Device Identity (SUDI) Certificates	Starting from Cisco IOS XE Dublin 17.12.1, the following changes have been introduced for trustpoints.
	• Trustpoint names for existing SUDI certificates
	If your device supports Cisco Manufacturing CA III certificate and is not disabled, the trustpoint names are as follows.
	• For *Cisco Manufacturing CA III* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA3_SUDI
	• For *Cisco Manufacturing CA SHA2* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA2_SUDI
	If your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled using **no platform sudi cmca3** command, the trustpoint names are as follows.
	• For *Cisco Manufacturing CA SHA2* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA2_SUDI
	• For *Cisco Manufacturing CA* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA_SUDI
	• Hardware SUDI certificates
	• If your device supports *High Assurance SUDI CA* certificate, this certificate is loaded under CISCO_IDEVID_SUDI trustpoint.
	• If your device does not support *High Assurance SUDI CA* certificate, *ACT2 SUDI CA* certificate is loaded under CISCO_IDEVID_SUDI trustpoint.
	• **show ip http server status** command output
	If you configure the trustpoint for the HTTP server as CISCO_IDEVID_SUDI, the output of **show ip http server status** command displays the operating trustpoint along with the configured trustpoint.
	The following example shows a sample output of **show ip http server status** command with both the configured and the operating trustpoint names. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the operating trustpoint in the below output displays CISCO_IDEVID_CMCA2_SUDI.
	`Device# show ip http server status`
	`…`
	`HTTP secure server trustpoint: CISCO_IDEVID_SUDI`
	`HTTP secure server operating trustpoint: CISCO_IDEVID_CMCA3_SUDI`
	(Network Essentials)

Feature Name	Description
Programmability: • NETCONF-SSH Algorithms • YANG Data Models	The following programmability features are introduced in this release: • NETCONF-SSH Algorithms: The NETCONF-SSH server configuration file contains the list of all supported algorithms. From this release onwards, you can enable or disable these algorithms at runtime by using Cisco IOS commands or YANG models. (Network Essentials) • 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/17121. (Network Advantage)
show idprom tan command	The **show idprom tan** command was introduced. It displays the top assembly part number and top assembly part revision number for the identification programmable read-only memory.

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

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.1

Behavior Change	Description
BDPU Guard and Root Guard Syslogs	The BDPU guard and root guard syslogs have been modified to include client bridge ID information.



CHAPTER 3

Important Notes

- Important Notes, on page 11

Important Notes

- Unsupported Feature
- Complete List of Supported Features
- Accessing Hidden Commands
- Default Behaviour

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 Behaviours

DF Bit Behavior for RADIUS Packets

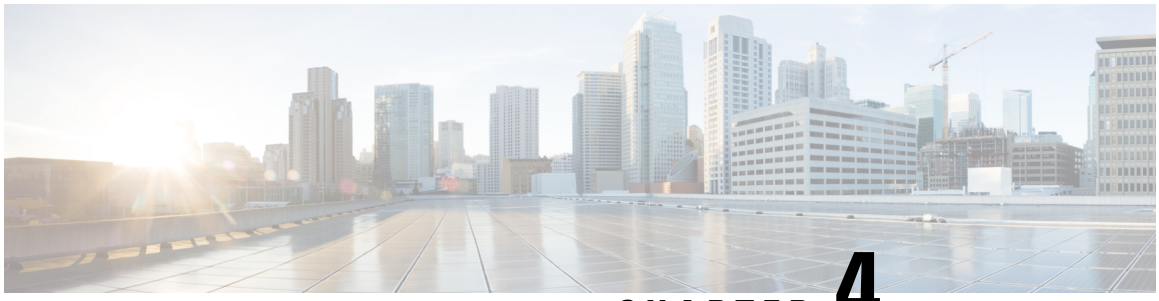
Beginning from Cisco IOS XE Gibraltar 16.12.5 and later, do not fragment bit (DF bit) in the IP packet is always set to 0 for all outgoing RADIUS packets (packets that originate from the device towards the RADIUS server).

Traffic Loss during during Stateful Switchover (SSO) and failover

On a Catalyst 9200 switch stack where traffic flows are ingressing on one switch and egressing on another, the following behavior is observed.

- If both ingress and egress are on member switches, the traffic drop is negligible (sub-second).
- If both ingress and egress are on hot standby switch (new active switch on failover), the traffic drop is negligible(sub-second).
- If ingress is on the active switch (being reloaded on failover) and egress is on the hot standby switch (new active switch on failover), the traffic drop lasts between 1 to 2 seconds.
- If both ingress and egress are on the active switch (being reloaded on failover), the traffic drop lasts between 3 to 8 seconds.
- The drop is observed irrespective of the Link Aggregation Control Protocol (LACP) rate.

Important Notes



CHAPTER 4

Compatibility Matrix and Web UI System Requirements

- Compatibility Matrix, on page 15
- Web UI System Requirements, 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.

Web UI System Requirements

The following subsections list the hardware and software required to access the Web UI:

Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1280 x 800 or higher	Small

1 We recommend 1 GHz
2 We recommend 1 GB DRAM

Software Requirements

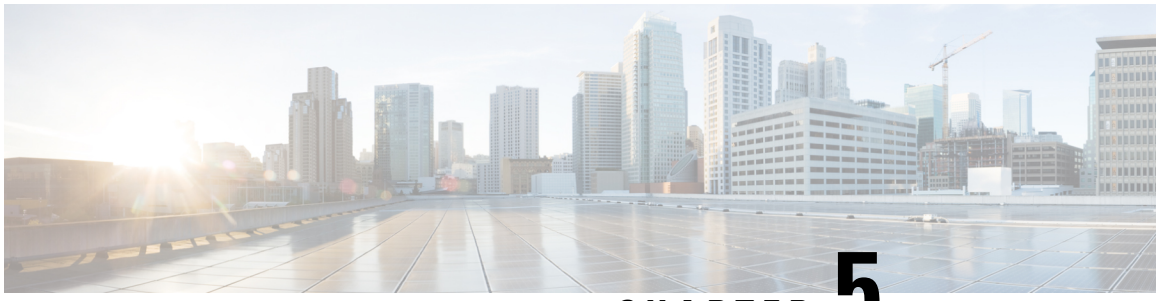
Operating Systems

- Windows 10 or later
- Mac OS X 10.9.5 or later

Browsers

- Google Chrome—Version 59 or later (On Windows and Mac)

- Microsoft Edge
- Mozilla Firefox—Version 54 or later (On Windows and Mac)
- Safari—Version 10 or later (On Mac)



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.

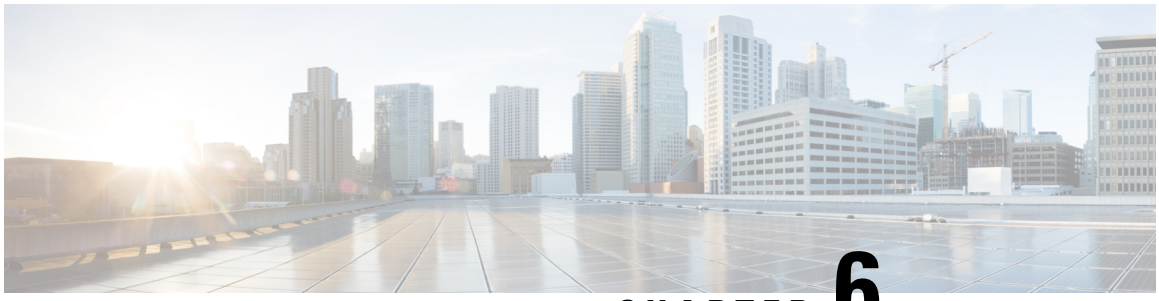
Available Licensing Models and Configuration Information

- 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 switched 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
```

- Catatyst 9000 Series Switches support MACsec switch-to-switch connections. We do not recommend configuring MACsec switch-to-host connections in an overlay network. For assistance with an existing switch-to-host MACsec implementation or a design review, contact your Cisco Sales Representative or Channel Partner.
- 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.
- Starting from Cisco IOS XE Release 17.10, the following Key Exchange and MAC algorithms are removed from the default list:

  Key Exchange algorithm:

  - diffie-hellman-group14-sha1

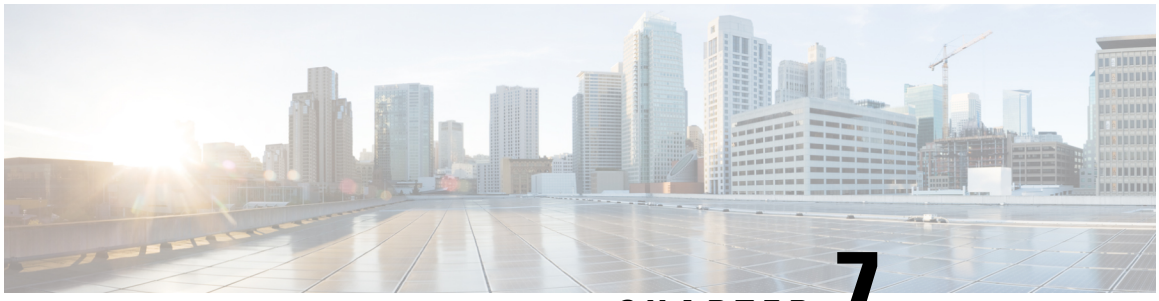
  MAC algorithms:

  - hmac-sha1
  - hmac-sha2-256
  - hmac-sha2-512



Note You can use the **ip ssh server algorithm kex** command to configure the Key Exchange algorithm and the **ip ssh server algorithm mac** command to configure the MAC algorithms.

Limitations and Restrictions



CHAPTER 7

Boot Loader Versions

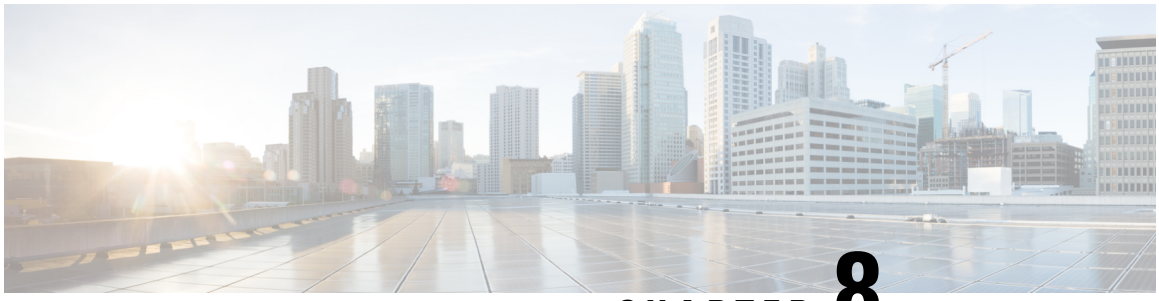
- Boot Loader Versions, on page 23

Boot Loader Versions

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

Release	ROMMON Version
Dublin 17.12.7a	17.12.1r [FC3]
Dublin 17.12.6	17.12.1r [FC3]
Dublin 17.12.5	17.12.1r [FC3]
Dublin 17.12.4	17.12.1r [FC3]
Dublin 17.12.3	17.12.1r [FC3]
Dublin 17.12.2	17.12.1r [FC3]
Dublin 17.12.1	17.12.1r [FC2]
Dublin 17.11.1	17.9.1r [FC11]
Dublin 17.10.1	17.9.1r [FC8]
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]

Release	ROMMON Version
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]
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 Dublin 17.12.7	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.12.07.SPA.bin
Cisco IOS XE Dublin 17.12.6	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.12.06.SPA.bin
Cisco IOS XE Dublin 17.12.5	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.12.05.SPA.bin
Cisco IOS XE Dublin 17.12.4	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.12.04.SPA.bin

Release	Image Type	File Name
Cisco IOS XE Dublin 17.12.3	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.12.03.SPA.bin
Cisco IOS XE Dublin 17.12.2	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.12.02.SPA.bin
Cisco IOS XE Dublin 17.12.1	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.12.01.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.

To know the bootloader version that applies to every major and maintenance release, see Boot Loader Versions, on page 23.

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 Dublin 17.11.x or earlier releases	Cisco IOS XE Dublin 17.12.x

The sample output in this section displays upgrade from Cisco IOS XE Dublin 17.11.1 to Cisco IOS XE Dublin 17.12.1 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 24 17:46:18 IST 2023
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.17.11.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.17.11.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.17.11.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.17.11.01.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.17.11.01.SPA.bin


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

[switch 1]:
```

```
Deleting file flash:cat9k_lite_iosxe.17.11.01.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 24 17:47:20 IST 2023
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.17.12.01.SPA.bin flash:

Destination filename [cat9k_lite_iosxe.17.12.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_lite_iosxe.17.12.01.SPA.bin...
Loading /cat9k_lite_iosxe.17.12.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]

601216545 bytes copied in 50.649 secs (11870255 bytes/sec)
```

b) **dir flash:**

Use this command to confirm that the image has been successfully copied to flash.

```
Switch# dir flash:*.bin
Directory of flash:/*.bin

Directory of flash:/

434184 -rw- 601216545 Jul 24 2023 10:18:11 -07:00 cat9k_lite_iosxe.17.12.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

Step 3 Set boot variable

a) **boot system flash:packages.conf**

Use this command to set the boot variable to **flash:packages.conf**.

```
Switch(config)# boot system flash:packages.conf
```

b) **no boot manual**

Use this command to configure the switch to auto-boot.

```
Switch(config)# no boot manual
Switch(config)# exit
```

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show boot**

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 Dublin 17.12.1 software image in the flash memory:

```
Switch# install add file flash:cat9k_lite_iosxe.17.12.01.SPA.bin activate commit
install_add_activate_commit: START Mon Jul 24 12:51:55 IST 2023
Jul 24 12:51:57.795: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
one-shot flash:cat9k_lite_iosxe.17.12.01.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.17.12.01.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: 17.12.01.0.276
install_add_activate_commit: Activating PACKAGE

gzip: initramfs.cpio.gz: decompression OK, trailing garbage ignored
Following packages shall be activated:
/flash/cat9k_lite-webui.17.12.01.SPA.pkg
/flash/cat9k_lite-srdriver.17.12.01.SPA.pkg
/flash/cat9k_lite-rpboot.17.12.01.SPA.pkg
/flash/cat9k_lite-rpbase.17.12.01.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 24 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.17.11.01.SPA.pkg
      Removed cat9k_lite-rpboot.17.11.01.SPA.pkg
      Removed cat9k_lite-srdriver.17.11.01.SPA.pkg
      Removed cat9k_lite-webui.17.11.01.SPA.pkg
    New files list:
      Added cat9k_lite-rpbase.17.12.01.SPA.pkg
      Added cat9k_lite-rpboot.17.12.01.SPA.pkg
      Added cat9k_lite-srdriver.17.12.01.SPA.pkg
      Added cat9k_lite-webui.17.12.01.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 24 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 24 13:04:23 IST 2023
Jul 24 13:04:24.586: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE flash:cat9k_lite_iosxe.17.12.01.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  Mar 9 2023 05:13:32 +00:00  cat9k_lite-rpbase.17.11.01.SPA.pkg
48585  -rw- 35713901   Mar 9 2023 05:14:12 +00:00  cat9k_lite-rpboot.17.11.01.SPA.pkg
48583  -rw- 4252692    Mar 9 2023 05:13:33 +00:00  cat9k_lite-srdriver.17.11.01.SPA.pkg
48584  -rw- 8119312    Mar 9 2023 05:13:34 +00:00  cat9k_lite-webui.17.11.01.SPA.pkg

16640  -rw- 301188116   Jul 24 2023 05:33:25 +00:00  cat9k_lite-rpbase.17.12.01.SPA.pkg
16647  -rw- 35112025    Jul 24 2023 05:34:06 +00:00  cat9k_lite-rpboot.17.12.01.SPA.pkg
16642  -rw- 4326420    Jul 24 2023 05:33:25 +00:00  cat9k_lite-srdriver.17.12.01.SPA.pkg
16643  -rw- 8328208     Jul 24 2023 05:33:25 +00:00  cat9k_lite-webui.17.12.01.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.17.12.01.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 24 2023 05:39:42 +00:00  packages.conf
16634 -rw- 4882  Jul 24 2023 05:34:06 +00:00  cat9k_lite_iosxe.17.12.01.SPA.conf
```

Step 6 Verify version

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 Dublin 17.12.1 image on the device:

```
Switch# show version

Cisco IOS XE Software, Version 17.12.01
Cisco IOS Software [Dublin], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 17.12.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2023 by Cisco Systems, Inc.
Compiled Mon 27-Mar-23 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 Dublin 17.12.x	Cisco IOS XE Dublin 17.11.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 Dublin 17.12.1 to Cisco IOS XE Dublin 17.11.1, 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 24 17:46:18 IST 2023
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.17.12.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.17.12.1.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.17.12.1.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.17.12.1.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.17.12.1.SPA.bin

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k_lite_iosxe.17.12.1.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 24 17:47:20 IST 2023
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.17.11.1.SPA.bin flash:

Destination filename [cat9k_lite_iosxe.17.11.1.SPA.bin]?
```

```
Accessing tftp://10.8.0.6//cat9k_lite_iosxe.17.11.1.SPA.bin...
Loading /cat9k_lite_iosxe.17.11.1.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 508584771 bytes]
508584771 bytes copied in 101.005 secs (5035244 bytes/sec)
```

b) **dir flash:**

Use this command to confirm that the image has been successfully copied to flash.

```
Switch# dir flash:*.bin
Directory of flash:/*.bin

Directory of flash:/

434184 -rw- 508584771 Mon Jul 24 2023 13:35:16 -07:00 cat9k_lite_iosxe.17.11.1.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Set boot variable

a) **boot system flash:packages.conf**

Use this command to set the boot variable to **flash:packages.conf**.

```
Switch(config)# boot system flash:packages.conf
```

b) **no boot manual**

Use this command to configure the switch to auto-boot.

```
Switch(config)# no boot manual
Switch(config)# exit
```

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show boot**

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 Downgrade software image

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 example displays the installation of the Cisco IOS XE Dublin 17.11.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_lite_iosxe.17.11.01.SPA.bin activate commit

install_add_activate_commit: START Mon Jul 24 13:17:28 IST 2023
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.17.11.01.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: 17.11.01.0.203
install_add_activate_commit: Activating PACKAGE

gzip: initramfs.cpio.gz: decompression OK, trailing garbage ignored
Following packages shall be activated:
/flash/cat9k_lite-webui.17.11.01.SPA.pkg
/flash/cat9k_lite-srdriver.17.11.01.SPA.pkg
/flash/cat9k_lite-rpboot.17.11.01.SPA.pkg
/flash/cat9k_lite-rpbase.17.11.01.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 24 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 24 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.17.12.01.SPA.pkg
      Removed cat9k_lite-rpboot.17.12.01.SPA.pkg
      Removed cat9k_lite-srdriver.17.12.01.SPA.pkg
      Removed cat9k_lite-webui.17.12.01.SPA.pkg
    New files list:
      Added cat9k_lite-rpbase.17.11.01.SPA.pkg
      Added cat9k_lite-rpboot.17.11.01.SPA.pkg
      Added cat9k_lite-srdriver.17.11.01.SPA.pkg
      Added cat9k_lite-webui.17.11.01.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 24 13:30:52 IST 2023
Jul 24 13:30:53.573: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE flash:cat9k_lite_iosxe.17.11.01.SPA.bin
Jul 24 13:30:53.573 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE flash:cat9k_lite_iosxe.17.11.01.SPA.bin

switch3#
Chassis 1 reloading, reason - Reload command

*Jul 24 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.17.11.01.SPA.bin
*Jul 24 13:30:54.526 IST: %STACKMGR-1-RELOAD: Switch 1 R0/0: stack_mgr: Reloading due to
reason Reload command Jul 24 13:30:58.121: %PMAN-5-EXITACTION: F0/0: pvp: Process manager
is exiting: reload fp actionrequested
Jul 24 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

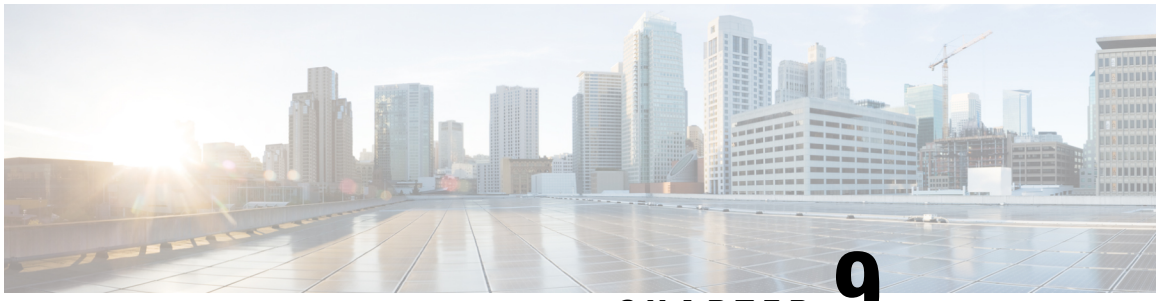
show version

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 Dublin 17.11.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.11.01
Cisco IOS Software [Dublin], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 17.11.1,
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2023 by Cisco Systems, Inc.
<output truncated>
```



CHAPTER 9

Caveats

- Cisco Bug Search Tool, on page 37
- Open Caveats in Cisco IOS XE Dublin 17.12.x, on page 37
- Resolved Caveats in Cisco IOS XE Dublin 17.12.7a, on page 38
- Resolved Caveats in Cisco IOS XE Dublin 17.12.6, on page 38
- Resolved Caveats in Cisco IOS XE Dublin 17.12.5, on page 38
- Resolved Caveats in Cisco IOS XE Dublin 17.12.4, on page 38
- Resolved Caveats in Cisco IOS XE Dublin 17.12.3, on page 39
- Resolved Caveats in Cisco IOS XE Dublin 17.12.2, on page 39
- Resolved Caveats in Cisco IOS XE Dublin 17.12.1, 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 Dublin 17.12.x

Identifier	Headline
CSCvu14870	Cat9k / Archive command causing 'bulk sync failure' and reloading Standby
CSCwh35728	Need switch to host macsec support in Sda overlay network

Resolved Caveats in Cisco IOS XE Dublin 17.12.7a

Identifier	Applicable Models	Headline
CSCwq22169	C9200	C9K switch unexpectedly reloads with FED crash due to memory corruption in the Stealth Watch Cloud (SWC) timer infra.
CSCws28363	C9200	9200 suddenly stops flow sending to SWC(uploading stuck)

Resolved Caveats in Cisco IOS XE Dublin 17.12.6

Identifier	Applicable Models	Headline
CSCwn85272	C9200L	9200L experiences linkdown on optical fiber link with C9606R

Resolved Caveats in Cisco IOS XE Dublin 17.12.5

Identifier	Headline
CSCwf34552	Switch is crashing during boot up and unable to upgrade 9200 stack
CSCwk27064	%SFF8472-3-READ_ERROR: Gi2/1/1: Error reading DOM data from transceiver
CSCwk44740	C9200L ifInDiscards always shows as 0 even though 'input queue drops' counter is increasing on gi0/0
CSCwk62333	Cat9200L Unexpected reload crimson db write lock held for too long
CSCwk76574	IPSG blocks traffic when client connect active switch in stack
CSCwk80732	Some of oid does not show output of MGMT port
CSCwk82261	Switch dropping TCP SYN packets <Random Port> DOT1X, MAB configuration

Resolved Caveats in Cisco IOS XE Dublin 17.12.4

Identifier	Applicable Models	Headline
CSCwk15432	C9200	Faulty PWR-C6-600WAC blocks PSU slot to recognize known wokring good PSU

Identifier	Applicable Models	Headline
CSCwj21346	C9200	C9200 Half-ring Stack, but the "Link OK" and "Sync OK" indicators show "yes"
CSCwk02145	C9200	C9200 Stack bandwidth is shown as N/A when the active side is down
CSCwk05581	C9200	C9200 Stack-ring speed remains at half-ring speed when the stack member is down
CSCwi32052	C9200	Endpoints lose network connection when macsec is enabled
CSCwj03295	C9200	GigabitEthernet ports connected to other Catalyst device go down when Switchover

Resolved Caveats in Cisco IOS XE Dublin 17.12.3

Identifier	Applicable Models	Headline
CSCwi30269	C9200	Port 2228 isn't closed after reload when l2-traceroute is disabled, Security threat
CSCwi62480	C9200	**show inventory** shows "Unknown uplink module" for FRU uplink module when reload Cat9200
CSCwi72959	C9200	When removed one FAN other FAN LED goes amber
CSCwh38627	C9200L	C9200L: Stack switch mgmt port reply unknon mac address
CSCwi60084	C9200L	Cat9200L may experience an Unexpected Reload
CSCwi06404	C9200	PKI crash after failing a CRL Fetch

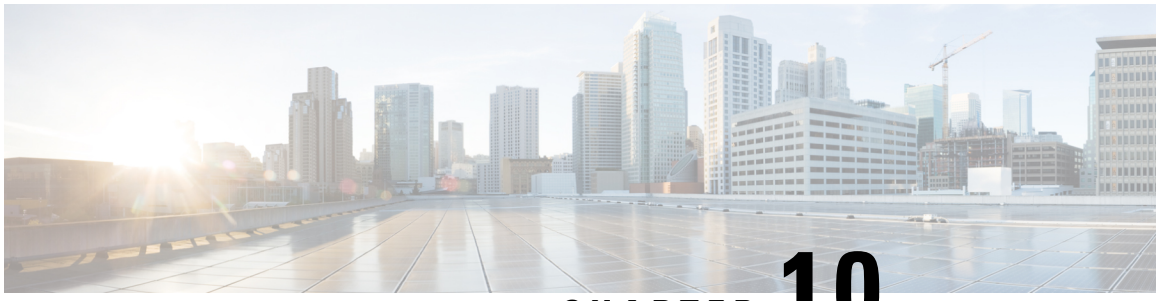
Resolved Caveats in Cisco IOS XE Dublin 17.12.2

Identifier	Applicable Models	Headline
CSCwf99608	C9200CX	Change AUX power value displayed in show env power for Changeup
CSCwf73002	C9200	Unable to remove port security configs under interface via netconf
CSCwf68913	C9200	C9000: Interface link flapping(down/up) occurs at Active Switch after switchover

Identifier	Applicable Models	Headline
CSCwh29961	C9200	show stacks: Information of Last System Crash:%Error opening crashinfo:crashinfo_RP_00_00
CSCwf78065	C9200	cat9200: CTS PAC download must fail when FIPS is enabled
CSCwh87343	All models	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.
CSCwh20734	C9200	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested&deleted
CSCwf18420	C9200	LLDP does not announce dynamically assigned VLAN

Resolved Caveats in Cisco IOS XE Dublin 17.12.1

Identifier	Headline
CSCwc41288	C9200L - Input Errors on Uplinks using 1G SFP
CSCwe47724	gbic-invalid error seen when connected CWDM-SFP-1610 and CWDM-SFP-1590 SFPs
CSCwe79864	9200: Incorrect Iout, pout and PS fan rpm speeds in "show env all" CLI



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)

© 2024 Cisco Systems, Inc. All rights reserved.