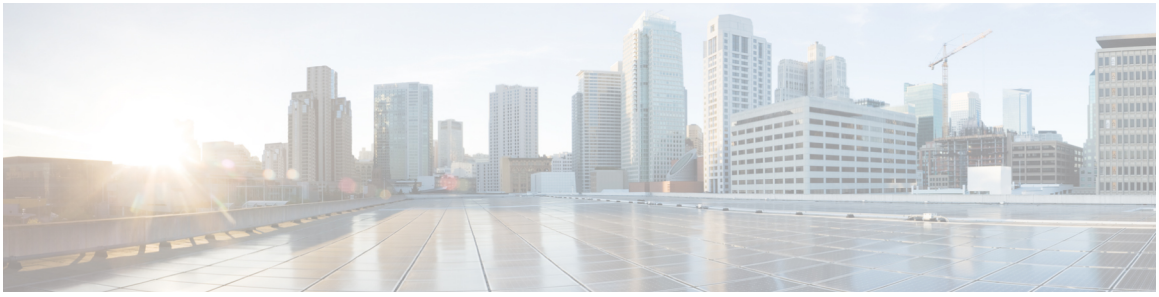


Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE 17.14.x

First Published: 2024-04-05

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



CONTENTS

CHAPTER 1 **Introduction** 1

Supported Hardware 1

Cisco Catalyst 9600 Series Switches—Model Numbers 1

Supported Hardware on Cisco Catalyst 9600 Series Switches 2

Optics Modules 4

CHAPTER 2 **What's New in Cisco IOS XE 17.14.x** 5

Hardware Features in Cisco IOS XE 17.14.1 5

Software Features in Cisco IOS XE 17.14.1 6

Hardware and Software Behavior Changes in Cisco IOS XE 17.14.1 7

CHAPTER 3 **Important Notes** 9

Important Notes 9

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 ROMMON Versions 23

ROMMON Versions 23

CHAPTER 8 Upgrading the Switch Software 27

Finding the Software Version 27

Software Images 27

Upgrading the ROMMON 28

Software Installation Commands 28

Upgrading in Install Mode 29

Downgrading in Install Mode 34

Field-Programmable Gate Array Version Upgrade 39

CHAPTER 9 Caveats 41

Cisco Bug Search Tool 41

Open Caveats in Cisco IOS XE 17.14.x 41

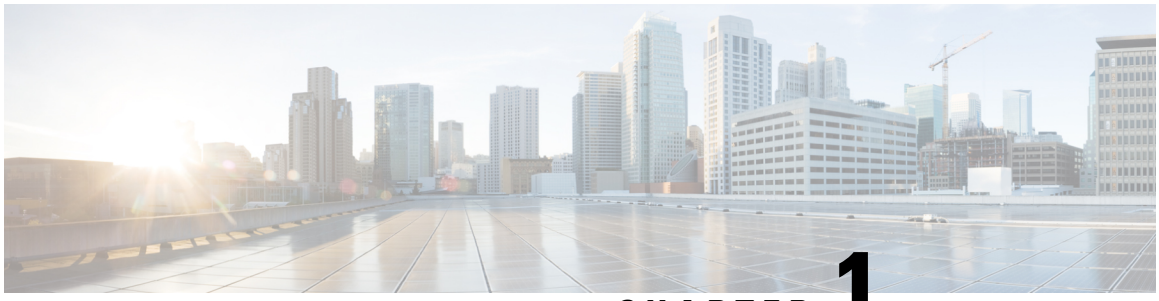
Resolved Caveats in Cisco IOS XE 17.14.1 41

CHAPTER 10 Additional Information 43

Troubleshooting 43

Related Documentation 43

Communications, Services, and Additional Information 43



CHAPTER 1

Introduction

Cisco Catalyst 9600 Series Switches are the next generation purpose-built 40 GigabitEthernet, 50 GigabitEthernet, 100 GigabitEthernet, and 400 GigabitEthernet modular core and aggregation platform providing resiliency at scale with the industry's most comprehensive security while allowing your business to grow at the lowest total operational cost. They have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

They deliver hardware and software convergence in terms of ASIC architecture with Unified Access Data Plane (UADP) 3.0 and Cisco Silicon One Q200. The platform runs an Open Cisco IOS XE that supports model driven programmability, Serial Advanced Technology Attachment (SATA) Solid State Drive (SSD) local storage, and a higher memory footprint). The series forms the foundational building block for SD-Access, which is Cisco's lead enterprise architecture.

It also supports features that provide high availability, advanced routing and infrastructure services, security capabilities, and application visibility and control.

• Supported Hardware, on page 1

Supported Hardware

Cisco Catalyst 9600 Series Switches—Model Numbers

The following table lists the supported switch models. For information about the available license levels, see section *License Levels*.

Switch Model (append with "=" for spares)	Description
C9606R	Cisco Catalyst 9606R Switch • Redundant supervisor module capability • Four linecard slots • Hot-swappable fan tray, front and rear serviceable, fan tray assembly with 9 fans. • Four power supply module slots

Supported Hardware on Cisco Catalyst 9600 Series Switches

Product ID (append with "=" for spares)	Description
Supervisor Modules	
C9600-SUP-1	Cisco Catalyst 9600 Series Supervisor 1 Module This supervisor module is supported on the C9606R chassis.
C9600X-SUP-2	Cisco Catalyst 9600 Series Supervisor Engine 2 This supervisor module is supported on the C9606R chassis.
SATA[1] SSD[2] Modules (for the Supervisor)	
C9K-F2-SSD-240GB	Cisco Catalyst 9600 Series 240GB SSD Storage
C9K-F2-SSD-480GB	Cisco Catalyst 9600 Series 480GB SSD Storage
C9K-F2-SSD-960GB	Cisco Catalyst 9600 Series 960GB SSD Storage
Line Cards	

C9600X-LC-56YL4C	Cisco Catalyst 9600 Series 56-Port SFP56, 4-Port QSFP28 line card.
	• C9600X-SUP-2
	  • 56 SFP56 ports of 50G/25G/10G
	  • 4 QSFP28 ports of 100G/40G
	• C9600-SUP-1
	  • Not supported

C9600X-LC-32CD	Cisco Catalyst 9600 Series 30-Port QSFP28, 2-Port QSFP-DD line card.
	• C9600X-SUP-2
	  • 30 QSFP28 ports of 100G/40G
	  • 2 QSFP-DD ports of 400G/200G/100G/40G
	• C9600-SUP-1
	  • Not supported

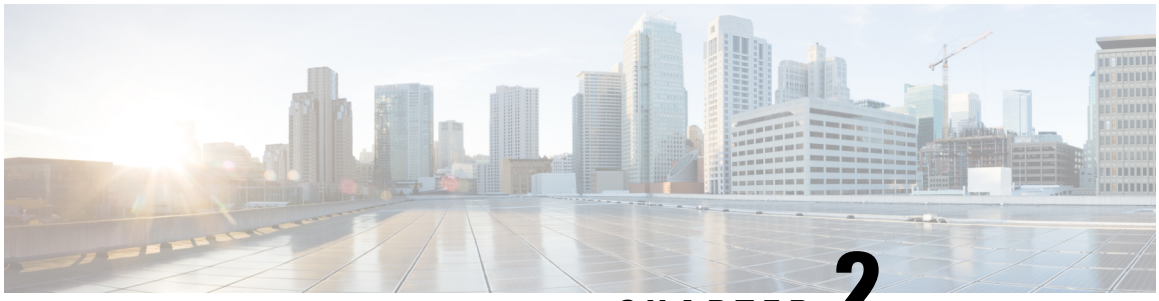
Product ID (append with "=" for spares)	Description
C9600-LC-40YL4CD	Cisco Catalyst 9600 Series 40-Port SFP56, 2-Port QSFP56, 2-Port QSFP-DD line card. • C9600X-SUP-2 • 40 SFP56 ports of 50G/25G/10G • 2 QSFP56 ports of 200G/100G/40G • 2 QSFP-DD ports of 400G/200G/100G/40G • C9600X-SUP-1 • 40 SFP28 ports of 25G/10G/1G • 2 QSFP28 ports of 100G/40G
C9600-LC-48YL	Cisco Catalyst 9600 Series 48-Port SFP56 line card. • C9600X-SUP-2 • 48 SFP56 ports of 50G/25G/10G • C9600X-SUP-1 • 48 SFP28 ports of 25G/10G/1G
C9600-LC-24C	Cisco Catalyst 9600 Series 24-Port 40G/12-Port 100G line card. • C9600X-SUP-2 • 24 QSFP28 ports of 100G/40G • C9600-SUP-1 • 12 ports of 100G or 24 ports of 40G
C9600-LC-48TX	Cisco Catalyst 9600 Series 48-Port MultiGigabit RJ45 line card. • C9600X-SUP-2 • 48 ports of 10G/5G/2.5G • C9600X-SUP-1 • 48 ports of 10G/5G/2.5G/1G and 100M/10M

Product ID (append with "=" for spares)	Description
C9600-LC-48S	Cisco Catalyst 9600 Series 48-Port SFP line card. • C9600X-SUP-2 • Not supported • C9600-SUP-1 • 48 SFP ports of 1G
AC Power Supply Modules	
C9600-PWR-2KWAC	Cisco Catalyst 9600 Series 2000W AC Power Supply Module[3]
C9600-PWR-3KWAC	Cisco Catalyst 9600 Series 3000W AC Power Supply Module
DC Power Supply Modules	
C9600-PWR-2KWDC	Cisco Catalyst 9600 Series 2000W DC Power Supply Module

1 Serial Advanced Technology Attachment (SATA)
2 Solid State Drive (SSD) Module
3 Power supply output capacity is 1050W at 110 VAC.

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 17.14.x

- Hardware Features in Cisco IOS XE 17.14.1, on page 5
- Software Features in Cisco IOS XE 17.14.1, on page 6
- Hardware and Software Behavior Changes in Cisco IOS XE 17.14.1, on page 7

Hardware Features in Cisco IOS XE 17.14.1

Feature Name	Description
Cisco SFP Modules for Gigabit Ethernet Applications	Supported transceiver module product numbers: • SFP-1G-LH • SFP-1G-SX Compatible line cards: • C9600-LC-40YL4CD, C9600-LC-48YL, and C9600X-LC-56YL4C line cards on Cisco Catalyst 9600X Supervisor Module 2 (C9600X-SUP-2) **Note** • A maximum of 24 SFP-1G-LH and/or SFP-1G-SX transceiver modules are supported per system. • SFP-1G-LH or SFP-1G-SX transceiver modules with CVR or QSA adapter on QSFP front panel ports are not supported. For information about the module, see Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Software Features in Cisco IOS XE 17.14.1

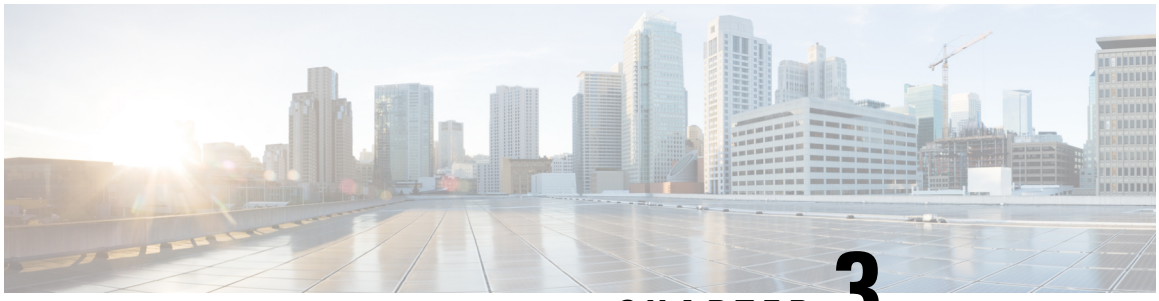
Feature Name	Description
BGP EVPN VXLAN • **fast-detection** command • **show lisp instance** {**ipv4** | **ipv6** | **ethernet**} command	The following BGP EVPN VXLAN features are introduced in this release: • **fast-detection** command: **fast-detection** command enables SD-Access support for fast wireless roaming of end points. • **show lisp instance** {**ipv4** | **ipv6** | **ethernet**} command: The output of **show lisp instance** {**ipv4** | **ipv6** | **ethernet**} command is enhanced to display the affinity ID for the local device.
IP SLA Probe Configuration Modification Capability	Introduces support to reconfigure the parameters of a scheduled IP SLA session using the **configure replace** command.
mDNS Protocol Options	The mDNS protocol option is introduced in the **device sensor filter spec** command. This allows the user to apply the mDNS protocol TLV filter list to the device sensor output. The **device sensor filter list mdns** command is introduced to create a mDNS protocol filter containing a list of Type-Length-Value (TLV) fields that can be included or excluded in the device sensor output. The **tlv** command is introduced to configure the list of Type Length Value (TLVs) in mDNS protocol configuration mode.
NAT SSO support with StackWise Virtual	Introduces support for synchronization of the NAT state information across active and standby devices so that if the active device fails, the standby device can take over smoothly and update its software without interrupting In-Service Software Upgrade (ISSU).
OSPF Local RIB Path Limit Enhancement	The OSPF Local RIB Path Limit feature is designed to restrict the number of paths stored by OSPF in its Local RIB, offering enhanced control over network path selection. With the **maximum-paths** command enabled, the network administrators can now control the number of paths OSPF installs in the Local RIB for a specific prefix. (Network Essentials and Network Advantage)

Feature Name	Description
Programmability: • gNMI: Stream Subscriptions with on-Change Mode • gNMI: SubscribeResponse with sync_response • YANG Data Models • YANG Support for Mutiple Next-Hops	The following programmability features are introduced in this release: • gNMI: Stream Subscriptions with on-Change Mode: gNMI telemetry supports on-change subscriptions on the same set of models as other telemetry protocols. (Network Essentials) • gNMI: SubscribeResponse with sync_response: The sync_response is a boolean field that is part of the SubscribeResponse response message. The sync_response message is sent after the first update message. (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/main/vendor/cisco/xe/17141. (Network Advantage) • YANG Support for Mutiple Next-Hops: A new container is added under the next-hop-options choice node to retrieve all next-hops for a given route or prefix. Also, an uptime leaf node is added to provide the timestamp for each next hop. (Network Advantage)
show reload history command	The **show reload history** command is introduced. It displays the reason for device reload and its history.

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

Hardware and Software Behavior Changes in Cisco IOS XE 17.14.1

Behavior Change	Description
Switch Integrated Security Features (SISF) – Enhanced Throttling Limit for ARP Packets	In Cisco IOS XE Amsterdam 17.3.1, a throttling limit was introduced to mitigate high CPU utilization scenarios. In a five second window, a maximum of 50 ARP broadcast packets per source IP were processed by SISF. In Cisco IOS XE 17.14.1, this limit is increased to a maximum of 100 ARP broadcast packets for each source IP. All ARP (ARP REQUEST and ARP REPLY) packets are dropped if • the limit is reached and • the security level of the device tracking policy is set to guard



CHAPTER 3

Important Notes

- Important Notes, on page 9

Important Notes

- Unsupported Features: Cisco Catalyst 9600 Series Supervisor 2 Module
- Complete List of Supported Features
- Accessing Hidden Commands
- Default Behaviour

Unsupported Features: Cisco Catalyst 9600 Series Supervisor 2 Module

- **BGP EVPN VXLAN**
  - Layer 2 Broadcast, Unknown Unicast, and Multicast (BUM) Traffic Forwarding using Ingress Replication
  - BUM Traffic Rate Limiting
  - Dynamic ARP inspection (DAI) and DHCP Rogue Server Protection
  - EVPN VXLAN Centralized Default Gateway
  - VXLAN-Aware Flexible Netflow
  - MPLS Layer 3 VPN Border Leaf Handoff
  - MPLS Layer 3 VPN Border Spine Handoff
  - VPLS over MPLS Border Leaf Handoff
  - VPLS over MPLS Border Spine Handoff
  - Interworking of Layer 3 TRM with MVPN Networks for IPv4 Traffic
  - Private VLANs (PVLANs)
  - BGP EVPN VXLAN with IPv6 in the Underlay (VXLANv6)
  - EVPN Microsegmentation

- VRF aware NAT64 EVPN Fabric
- EVPN VXLAN Multi-Homing

- **Cisco TrustSec**
  - Cisco TrustSec Security Association Protocol (SAP)
  - Cisco TrustSec SGT Caching

- **High Availability**
  - Quad-Supervisor with Route Processor Redundancy
  - Secure StackWise Virtual

- **Interface and Hardware**
  - Link Debounce Timer
  - EnergyWise

- **IP Addressing Services**
  - Next Hop Resolution Protocol (NHRP)
  - Network Address Translation (NAT)
  - Gateway Load Balancing Protocol (GLBP)
  - Web Cache Communication Protocol (WCCP)
  - Switchport Block Unknown Unicast and Switchport Block Unknown Multicast
  - Message Session Relay Protocol (MSRP)
  - TCP MSS Adjustment

- **IP Multicast Routing**
  - Multicast Routing over GRE Tunnel
  - Multicast VLAN Registration (MVR) for IGMP Snooping
  - IPv6 Multicast over Point-to-Point GRE
  - IGMP Proxy
  - Bidirectional PIM
  - Multicast VPN
  - MVPNv6
  - mVPN Extranet Support
  - MLDP-Based VPN
  - PIM Snooping
  - PIM Dense Mode

- **IP Routing**
  - OSPFv2 Loop-Free Alternate IP Fast Reroute
  - EIGRP Loop-Free Alternate IP Fast Reroute
  - PBR for Object-Group Access Control List (OGACL) Based Matching
  - Multipoint GRE
  - Unicast and Multicast over Point-to-Multipoint GRE
  - GRE IPv6 Tunnels
  - IP Fast Reroute (IP FRR)
- **Layer 2**
  - Loop Detection Guard
  - Multi-VLAN Registration Protocol (MVRP)
  - Precision Time Protocol (PTP)
  - Resilient Ethernet Protocol
- **Multiprotocol Label Switching**
  - LAN MACsec over Multiprotocol Label Switching (MPLS)
  - BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN
  - MPLS over GRE
  - MPLS Layer 2 VPN over GRE
  - MPLS Layer 3 VPN over GRE
  - Virtual Private LAN Service (VPLS)
  - VPLS Autodiscovery, BGP-based
  - VPLS Layer 2 Snooping: Internet Group Management Protocol or Multicast Listener Discovery
  - Hierarchical VPLS with MPLS Access
  - VPLS Routed Pseudowire IRB(v4) Unicast
  - MPLS VPN Inter-AS Options (options B and AB)
  - MPLS VPN Inter-AS IPv4 BGP Label Distribution
  - Seamless Multiprotocol Label Switching
- **Network Management**
  - Flow-Based Switch Port Analyser
  - RSPAN
  - FRSPAN

- Egress Netflow
- IP Aware MPLS Netflow
- NetFlow Version 5

- **Quality of Service**
  - QoS Ingress Shaping
  - VPLS QoS
  - Microflow Policers
  - Per VLAN Policy and Per Port Policer
  - Mixed COS/DSCP Threshold in a QoS LAN-queueing Policy
  - Easy QoS: match-all Attributes
  - Classify: Packet Length
  - Class-Based Shaping for DSCP/Prec/COS/MPLS Labels
  - CoPP Microflow Policing
  - Egress Policing
  - Egress Microflow Destination-Only Policing
  - Ethertype Classification
  - Packet Classification Based on Layer3 Packet-Length
  - PACLs
  - Per IP Session QoS
  - Per Queue Policer
  - QoS Data Export
  - QoS L2 Missed Packets Policing

- **Security**
  - Lawful Intercept
  - MACsec:
    - MACsec EAP-TLS
    - Switch-to-host MACsec
    - Certificate-based MACsec
    - Cisco TrustSec SAP MACsec
  - MAC ACLs
  - Port ACLs

- VLAN ACLs
- IP Source Guard
- IPv6 Source Guard
- Web-based Authentication
- Port Security
- Weighted Random Early Detection mechanism (WRED) Based on DSCP, PREC, or COS
- IEEE 802.1x Port-Based Authentication
- Dynamic ARP Inspection
- Dynamic ARP Inspection Snooping

- **System Management**
  - Unicast MAC Address Filtering
- **VLAN**
  - Wired Dynamic PVLAN
  - Private VLANs

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.

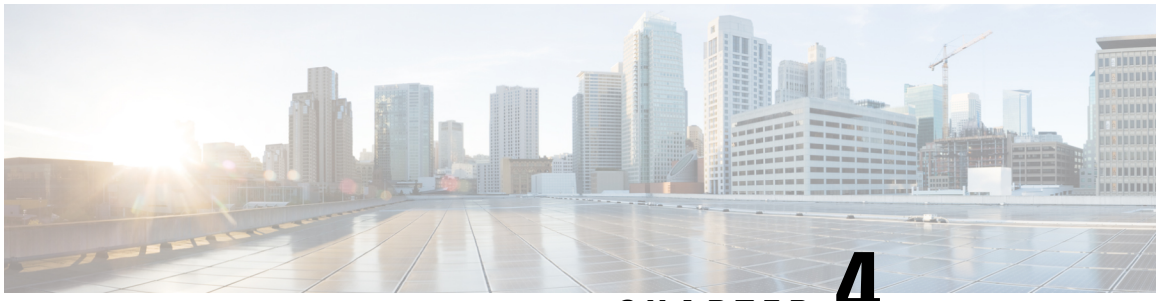


Important We recommend that you use any hidden command only under TAC supervision.

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 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).



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 9600 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[4]	512 MB[5]	256	1280 x 800 or higher	Small

[4] We recommend 1 GHz
[5] We recommend 1 GB DRAM

Software Requirements

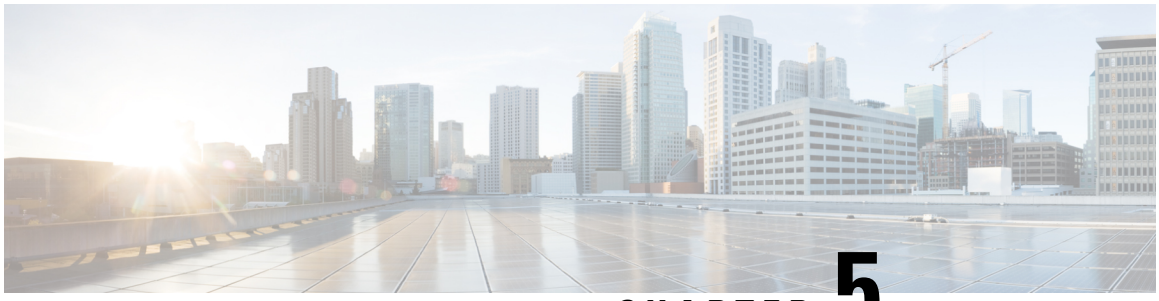
Operating Systems

- 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 Gibraltar 16.11.1 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.

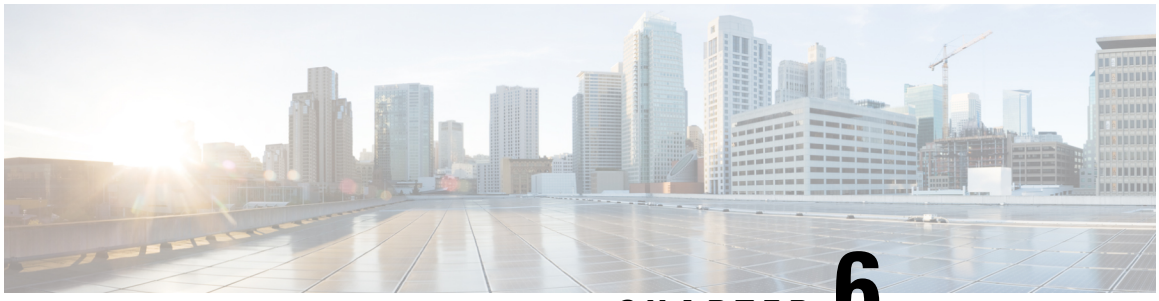
Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst 9600 Series Switches datasheets at:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-series-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-series-line-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-ser-sup-eng-data-sheet-cte-en.html



CHAPTER 6

Limitations and Restrictions

- Limitations and Restrictions, on page 19

Limitations and Restrictions

- Auto negotiation: The SFP+ interface (TenGigabitEthernet0/1) on the Ethernet management port with a 1G transceiver does not support auto negotiation.
- 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.
- Convergence: During SSO, a higher convergence time is observed while removing the active supervisor module installed in slot 3 of a C9606R chassis.
- Cisco Catalyst 9600 Series Supervisor 2 Module (C9600X-SUP-2) on a C9606R chassis does not support Quad-Supervisor with RPR.
- Hardware Limitations—Optics:
  - Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapter —This adapter must not be installed on an even numbered port where the corresponding odd numbered port is configured as 40GE port. For example, if port 1 is configured as 40GE, CVR-QSFP-SFP10G must not be installed in port 2.

    Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapter — If you insert a 40-Gigabit Ethernet Transceiver Module to odd numbered port, the corresponding even numbered port does not work with CVR-QSFP-SFP10G adapter.
  - GLC-T and GLC-TE operating at 10/100Mbps speed are not supported with Cisco QSA Module (CVR-QSFP-SFP10G).
  - SFP-10G-T-X supports 100Mbps/1G/10G speeds based on auto negotiation with the peer device. You cannot force speed settings from the transceiver.
- Hardware Limitations—Power Supply Modules:
  - Input voltage for AC power supply modules—All AC-input power supply modules in the chassis must have the same AC-input voltage level.

- Using power supply modules of different types—When mixing AC-input and DC-input power supplies, the AC-input voltage level must be 220 VAC.

- In-Service Software Upgrade (ISSU)
  - Within a major release train (16.x or 17.x or 18.x), ISSU is supported between any two EMs that are released not more than 3 years apart.
  - Within a major release train, ISSU is supported from:
    - Any EM (EM1, EM2, EM3) to another EM (EM1, EM2, EM3)

      Example: 16.9.x to 16.12.x, 17.3.x to 17.6.x, 17.6.x to 17.9.x
    - Any release within the same EM

      Example: 16.9.2 to 16.9.3 or 16.9.4 or 16.9.x, 16.12.1 to 16.12.2 or 16.12.3 or 16.12.x, 17.3.1 to 17.3.2 or 17.3.3 or 17.3.x
  - Between major release trains, ISSU is not supported from:
    - An EM of a major release train to an EM of another major release train

      Example: 16.x.x to 17.x.x or 17.x.x to 18.x.x is not supported
    - An SM to EM or EM to SM

      Example: 16.10.x or 16.11.x to 16.12.x is not supported
  - ISSU is not supported on engineering special releases and .s (or similar) images.
  - ISSU is not supported between Licensed Data Payload Encryption (LDPE) and No Payload Encryption (NPE) Cisco IOS XE software images.
  - ISSU downgrades are not supported.
  - While ISSU allows you to perform upgrades with zero downtime, we recommend you to do so during a maintenance window only.
  - If a new feature introduced in a software release requires a change in configuration, the feature should not be enabled during ISSU.
  - If a feature is not available in the downgraded version of a software image, the feature should be disabled before initiating ISSU.

- 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.

- 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.

- On the Cisco Catalyst 9600 Series Supervisor 2 Module, TCAM space will not be reserved for different features. The available TCAM space will be shared across the features.

- The File System Check (fsck) utility is not supported in install mode.

- The command **service-routing mdns-sd** is being deprecated. Use the **mdns-sd gateway** command instead.

- 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:

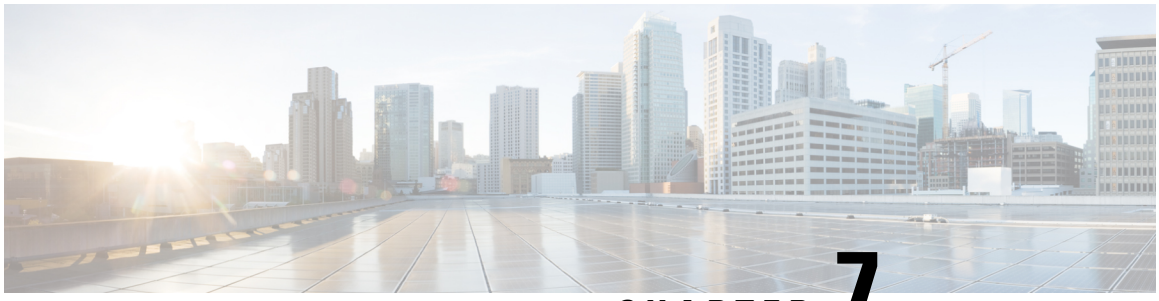
  - diffie-hellman-group14-sha1

  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.



CHAPTER 7

ROMMON Versions

- ROMMON Versions, on page 23

ROMMON Versions

ROMMON, also known as the boot loader, is firmware that runs when the device is powered up or reset. It initializes the processor hardware and boots the operating system software (Cisco IOS XE software image). The ROMMON is stored on the following Serial Peripheral Interface (SPI) flash devices on your switch:

- Primary: The ROMMON stored here is the one the system boots every time the device is powered-on or reset.
- Golden: The ROMMON stored here is a backup copy. If the one in the primary is corrupted, the system automatically boots the ROMMON in the golden SPI flash device.

ROMMON upgrades may be required to resolve firmware defects, or to support new features, but there may not be new versions with every release.

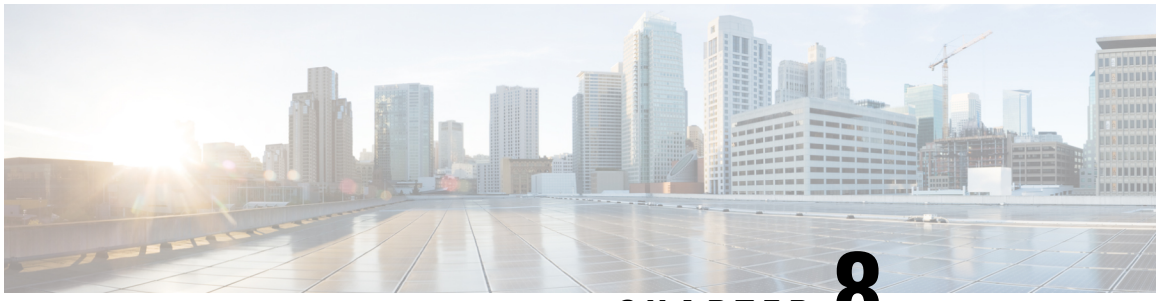
The following table provides ROMMON version information for the Cisco Catalyst 9600 Series Supervisor Modules. For ROMMON version information of Cisco IOS XE 16.x.x releases, refer to the corresponding Cisco IOS XE 16.x.x release notes of the respective platform.

Release	ROMMON Version (C9600-SUP-1)	ROMMON Version (C9600X-SUP-2)
17.14.1	17.8.1r[FC1]	17.10.1r
17.13.1	17.8.1r[FC1]	17.10.1r
Dublin 17.12.7a	17.8.1r[FC1]	17.10.1r
Dublin 17.12.6	17.8.1r[FC1]	17.10.1r
Dublin 17.12.5	17.8.1r[FC1]	17.10.1r
Dublin 17.12.4	17.8.1r[FC1]	17.10.1r
Dublin 17.12.3	17.8.1r[FC1]	17.10.1r
Dublin 17.12.2	17.8.1r[FC1]	17.10.1r
Dublin 17.12.1	17.8.1r[FC1]	17.10.1r

Release	ROMMON Version (C9600-SUP-1)	ROMMON Version (C9600X-SUP-2)
Dublin 17.11.1	17.8.1r[FC1]	17.10.1r
Dublin 17.10.1	17.8.1r[FC1]	17.10.1r
Cupertino 17.9.9	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.8	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.7	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.6a	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.6	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.5	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.4	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.3	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.2	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.1	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.8.1	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.7.1	17.6.1r	17.7.1r[FC3]
Bengaluru 17.6.8	17.6.1r	-
Bengaluru 17.6.7	17.6.1r	-
Bengaluru 17.6.6a	17.6.1r	-
Bengaluru 17.6.6	17.6.1r	-
Bengaluru 17.6.5	17.6.1r	-
Bengaluru 17.6.4	17.6.1r	-
Bengaluru 17.6.3	17.6.1r	-
Bengaluru 17.6.2	17.6.1r	-
Bengaluru 17.6.1	17.6.1r	-
Bengaluru 17.5.1	17.3.1r[FC2]	-
Bengaluru 17.4.1	17.3.1r[FC2]	-
Amsterdam 17.3.8a	17.3.1r[FC2]	-
Amsterdam 17.3.8	17.3.1r[FC2]	-
Amsterdam 17.3.7	17.3.1r[FC2]	-

Release	ROMMON Version (C9600-SUP-1)	ROMMON Version (C9600X-SUP-2)
Amsterdam 17.3.6	17.3.1r[FC2]	-
Amsterdam 17.3.5	17.3.1r[FC2]	-
Amsterdam 17.3.4	17.3.1r[FC2]	-
Amsterdam 17.3.3	17.3.1r[FC2]	-
Amsterdam 17.3.2a	17.3.1r[FC2]	-
Amsterdam 17.3.1	17.3.1r[FC2]	-
Amsterdam 17.2.1	17.1.1[FC2]	-
Amsterdam 17.1.1	17.1.1[FC1]	-

ROMMON Versions



CHAPTER 8

Upgrading the Switch Software

- Finding the Software Version, on page 27
- Software Images, on page 27
- Upgrading the ROMMON, on page 28
- Software Installation Commands, on page 28
- Upgrading in Install Mode, on page 29
- Downgrading in Install Mode, on page 34
- Field-Programmable Gate Array Version Upgrade, on page 39

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 17.14.1	CAT9K_IOSXE	cat9k_iosxe.17.14.01.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.14.01.

Upgrading the ROMMON

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

You can upgrade the ROMMON before, or, after upgrading the software version. If a new ROMMON version is available for the software version you are upgrading to, proceed as follows:

- Upgrading the ROMMON in the primary SPI flash device

  This ROMMON is upgraded automatically. When you upgrade from an existing release on your switch to a later or newer release for the first time, and there is a new ROMMON version in the new release, the system automatically upgrades the ROMMON in the primary SPI flash device, based on the hardware version of the switch.

- Upgrading the ROMMON in the golden SPI flash device

  You must manually upgrade this ROMMON. Enter the **upgrade rom-monitor capsule golden switch** command in privileged EXEC mode.

Note

- In case of a Cisco StackWise Virtual setup, upgrade the active and standby supervisor modules.
- In case of a High Availability set up, upgrade the active and standby supervisor modules.

After the ROMMON is upgraded, it will take effect on the next reload. If you go back to an older release after this, the ROMMON is not downgraded. The updated ROMMON supports all previous releases.

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.

Summary of Software Installation Commands	
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, using **install** commands, in install mode. To perform a software image upgrade, you must be booted into IOS through **boot flash:packages.conf**.

Before you begin

Caution You must comply with these cautionary guidelines during an upgrade:

- Do not power cycle the switch.
- Do not disconnect power or remove the supervisor module.
- Do not perform an online insertion and replacement (OIR) of either supervisor (in a High Availability setup), if one of the supervisor modules in the chassis is in the process of a bootloader upgrade or when the switch is booting up.
- Do not perform an OIR of a switching module (linecard) when the switch is booting up.

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

When upgrading from ...	To...
Cisco IOS XE 17.13.x or earlier releases	Cisco IOS XE 17.14.x

The sample output in this section displays upgrade from Cisco IOS XE 17.13.1 to Cisco IOS XE 17.14.1 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 Mar 25 19:51:48 UTC 2024
```

```
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
    cat9k-cc_srdriver.17.13.01.SPA.pkg
      File is in use, will not delete.
    cat9k-espbase.17.13.01.SPA.pkg
      File is in use, will not delete.
    cat9k-guestshell.17.13.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpbase.17.13.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpboot.17.13.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipbase.17.13.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipspa.17.13.01.SPA.pkg
      File is in use, will not delete.
    cat9k-srdriver.17.13.01.SPA.pkg
      File is in use, will not delete.
    cat9k-webui.17.13.01.SPA.pkg
      File is in use, will not delete.
    cat9k-wlc.17.13.01.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-cc_srdriver.17.13.01.SPA.pkg
/flash/cat9k-espbase.17.13.01.SPA.pkg
/flash/cat9k-guestshell.17.13.01.SPA.pkg
/flash/cat9k-rpbase.17.13.01.SPA.pkg
/flash/cat9k-rpboot.17.13.01.SPA.pkg
/flash/cat9k-sipbase.17.13.01.SPA.pkg
/flash/cat9k-sipspa.17.13.01.SPA.pkg
/flash/cat9k-srdriver.17.13.01.SPA.pkg
/flash/cat9k-webui.17.13.01.SPA.pkg
/flash/cat9k-wlc.17.13.01.SPA.pkg
/flash/packages.conf

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

[switch 1]:
Deleting file flash:cat9k-cc_srdriver.17.13.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.17.13.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.17.13.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.17.13.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.13.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.17.13.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.17.13.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.17.13.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.17.13.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.17.13.01.SPA.pkg ... done.
Deleting file flash:packages.conf ... 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 Mar 25 19:52:25 UTC 2024
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_iosxe.17.14.01.SPA.bin flash:

destination filename [cat9k_iosxe.17.14.01.SPA.bin]?
Accessing tftp://10.8.0.6/image/cat9k_iosxe.17.14.01.SPA.bin...
Loading /cat9k_iosxe.17.14.01.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:*.bin**

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    Mar 25 2024 10:18:11 -07:00 cat9k_iosxe.17.14.01.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. Settings are synchronized with the standby switch, if applicable.

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

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show bootvar**

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

```
Switch# show bootvar
BOOT variable = bootflash:packages.conf
MANUAL_BOOT variable = no
```

```
BAUD variable = 9600
ENABLE_BREAK variable = yes
BOOTMODE variable does not exist
IPXE_TIMEOUT variable does not exist
CONFIG_FILE variable =

Standby BOOT variable = bootflash:packages.conf
Standby MANUAL_BOOT variable = no
Standby BAUD variable = 9600
Standby ENABLE_BREAK variable = yes
Standby BOOTMODE variable does not exist
Standby IPXE_TIMEOUT variable does not exist
Standby CONFIG_FILE variable =
```

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 a TFTP server or the flash , if you have copied the image to flash memory.

The following sample output displays installation of the Cisco IOS XE 17.14.1 software image to flash:

```
Switch# install add file flash:cat9k_iosxe.17.14.01.SPA.bin activate commit
_install_add_activate_commit: START Mon Mar 25 16:37:25 IST 2024

*Mar 25 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.17.14.01.SPA.bin
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

This operation requires a reload of the system. Do you want to proceed?
Please confirm you have changed boot config to flash:packages.conf [y/n]y

--- Starting initial file syncing ---
Copying image file: flash:cat9k_iosxe.17.14.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.14.01.SPA.bin to standby
Finished initial file syncing

--- Starting Add ---
Performing Add on Active/Standby
  [R0] Add package(s) on R0
  [R0] Finished Add on R0
  [R1] Add package(s) on R1
  [R1] Finished Add on R1
Checking status of Add on [R0 R1]
Add: Passed on [R0 R1]
Finished Add

Image added. Version: 17.14.01

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.14.01.SPA.pkg
/flash/cat9k-webui.17.14.01.SPA.pkg
/flash/cat9k-srdriver.17.14.01.SPA.pkg
/flash/cat9k-sipspa.17.14.01.SPA.pkg
/flash/cat9k-sipbase.17.14.01.SPA.pkg
/flash/cat9k-rpboot.17.14.01.SPA.pkg
/flash/cat9k-rpbase.17.14.01.SPA.pkg
/flash/cat9k-guestshell.17.14.01.SPA.pkg
/flash/cat9k-espbase.17.14.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.14.01.SPA.pkg
```

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

--- Starting Activate ---
Performing Activate on Active/Standby
*Mar 25 16:45:21.695 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds  [R0] Activate package(s) on R0
  [R0] Finished Activate on R0
  [R1] Activate package(s) on R1
  [R1] Finished Activate on R1
Checking status of Activate on [R0 R1]
Activate: Passed on [R0 R1]
Finished Activate

*Mar 25 16:45:25.233 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R1/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds--- Starting Commit ---
Performing Commit on Active/Standby
  [R0] Commit package(s) on R0
  [R0] Finished Commit on R0
  [R1] Commit package(s) on R1
  [R1] Finished Commit on R1
Checking status of Commit on [R0 R1]
Commit: Passed on [R0 R1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Mon Mar 25 16:46:18 IST 2024
```

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 the **dir flash:** command to verify that the flash partition has ten new `.pkg` files and two `.conf` files.

a) **dir flash:*.conf**

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

```
Switch# dir flash:*.pkg
Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104    Nov 20 2023 09:52:41 -07:00 cat9k-cc_srdriver.17.13.01.SPA.pkg
475141 -rw- 70333380   Nov 20 2023 09:52:44 -07:00 cat9k-espbase.17.13.01.SPA.pkg
475142 -rw- 13256      Nov 20 2023 09:52:44 -07:00 cat9k-guestshell.17.13.01.SPA.pkg
475143 -rw- 349635524  Nov 20 2023 09:52:54 -07:00 cat9k-rpbase.17.13.01.SPA.pkg
475149 -rw- 24248187   Nov 20 2023 09:53:02 -07:00 cat9k-rpboot.17.13.01.SPA.pkg
475144 -rw- 25285572   Nov 20 2023 09:52:55 -07:00 cat9k-sipbase.17.13.01.SPA.pkg
475145 -rw- 20947908   Nov 20 2023 09:52:55 -07:00 cat9k-sipspa.17.13.01.SPA.pkg
475146 -rw- 2962372    Nov 20 2023 09:52:56 -07:00 cat9k-srdriver.17.13.01.SPA.pkg
475147 -rw- 13284288   Nov 20 2023 09:52:56 -07:00 cat9k-webui.17.13.01.SPA.pkg
475148 -rw- 13248      Nov 20 2023 09:52:56 -07:00 cat9k-wlc.17.13.01.SPA.pkg

491524 -rw- 25711568   Mar 25 2024 11:49:33 -07:00  cat9k-cc_srdriver.17.14.01.SPA.pkg
491525 -rw- 78484428   Mar 25 2024 11:49:35 -07:00  cat9k-espbase.17.14.01.SPA.pkg
491526 -rw- 1598412    Mar 25 2024 11:49:35 -07:00  cat9k-guestshell.17.14.01.SPA.pkg
491527 -rw- 404153288  Mar 25 2024 11:49:47 -07:00  cat9k-rpbase.17.14.01.SPA.pkg
491533 -rw- 31657374   Mar 25 2024 11:50:09 -07:00  cat9k-rpboot.17.14.01.SPA.pkg
491528 -rw- 27681740   Mar 25 2024 11:49:48 -07:00  cat9k-sipbase.17.14.01.SPA.pkg
491529 -rw- 52224968   Mar 25 2024 11:49:49 -07:00  cat9k-sipspa.17.14.01.SPA.pkg
491530 -rw- 31130572   Mar 25 2024 11:49:50 -07:00  cat9k-srdriver.17.14.01.SPA.pkg
491531 -rw- 14783432   Mar 25 2024 11:49:51 -07:00  cat9k-webui.17.14.01.SPA.pkg
```

```
491532 -rw- 9160       Mar 25 2024 11:49:51 -07:00  cat9k-wlc.17.14.01.SPA.pkg

11353194496 bytes total (8963174400 bytes free)
```

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_iosxe.17.14.01.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 Mar 25 2024 05:39:42 +00:00  packages.conf
16634  -rw- 4882 Mar 25 2024 05:34:06 +00:00  cat9k_iosxe.17.14.01.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 17.14.1 image on the device:

```
Switch# show version

Cisco IOS XE Software, Version 17.14.01
Cisco IOS Software, Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.14.1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2024 by Cisco Systems, Inc..
<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 17.14.x	Cisco IOS XE 17.13.x or earlier releases.

Note New switch models that are introduced in a release cannot be downgraded. The release in which a module is introduced is the minimum software version for that model. We recommend upgrading all existing hardware to the same release as the latest hardware.

The sample output in this section shows downgrade from Cisco IOS XE 17.14.1 to Cisco IOS XE 17.13.1, 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 Nov 20 11:42:27 IST 2023

Cleaning up unnecessary package files

No path specified, will use booted path bootflash:packages.conf

Cleaning bootflash:
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat9k-cc_srdriver.17.14.01.SSA.pkg
      File is in use, will not delete.
    cat9k-espbase.17.14.01.SSA.pkg
      File is in use, will not delete.
    cat9k-guestshell.17.14.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpbase.17.14.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpboot.17.14.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipbase.17.14.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipspa.17.14.01.SSA.pkg
      File is in use, will not delete.
    cat9k-srdriver.17.14.01.SSA.pkg
      File is in use, will not delete.
    cat9k-webui.17.14.01.SSA.pkg
      File is in use, will not delete.
    cat9k-wlc.17.14.01.SSA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.
SUCCESS: No extra package or provisioning files found on media. Nothing to clean.

SUCCESS: install_remove  Mon Nov 20 11:42:39 IST 2023

--- 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 Nov 20 19:52:25 UTC 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_iosxe.17.13.01.SPA.bin flash:
Destination filename [cat9k_iosxe.17.13.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.17.13.01.SPA.bin...
Loading /cat9k_iosxe.17.13.01.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 Nov 20 2023 13:35:16 -07:00 cat9k_iosxe.17.13.01.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. Settings are synchronized with the standby switch, if applicable.

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

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show bootvar**

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

```
Switch# show bootvar
BOOT variable = bootflash:packages.conf
MANUAL_BOOT variable = no
BAUD variable = 9600
ENABLE_BREAK variable = yes
BOOTMODE variable does not exist
IPXE_TIMEOUT variable does not exist
CONFIG_FILE variable =

Standby BOOT variable = bootflash:packages.conf
Standby MANUAL_BOOT variable = no
Standby BAUD variable = 9600
Standby ENABLE_BREAK variable = yes
Standby BOOTMODE variable does not exist
Standby IPXE_TIMEOUT variable does not exist
Standby CONFIG_FILE variable =
```

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 a TFTP server or the flash , if you have copied the image to flash memory.

The following example displays the installation of the Cisco IOS XE 17.13.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.17.13.01.SPA.bin activate commit
_install_add_activate_commit: START Mon Nov 20 21:37:25 IST 2023

*Nov 20 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.17.13.01.SPA.bin
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

This operation requires a reload of the system. Do you want to proceed?
Please confirm you have changed boot config to flash:packages.conf [y/n]y

--- Starting initial file syncing ---
Copying image file: flash:cat9k_iosxe.17.13.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.13.01.SPA.bin to standby
Finished initial file syncing

--- Starting Add ---
Performing Add on Active/Standby
  [R0] Add package(s) on R0
  [R0] Finished Add on R0
  [R1] Add package(s) on R1
  [R1] Finished Add on R1
Checking status of Add on [R0 R1]
Add: Passed on [R0 R1]
Finished Add

Image added. Version: 17.13.1
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.13.01.SPA.pkg
/flash/cat9k-webui.17.13.01.SPA.pkg
/flash/cat9k-srdriver.17.13.01.SPA.pkg
/flash/cat9k-sipspa.17.13.01.SPA.pkg
/flash/cat9k-sipbase.17.13.01.SPA.pkg
/flash/cat9k-rpboot.17.13.01.SPA.pkg
```

```
/flash/cat9k-rpbase.17.13.01.SPA.pkg
/flash/cat9k-guestshell.17.13.01.SPA.pkg
/flash/cat9k-espbase.17.13.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.13.01.SPA.pkg

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

--- Starting Activate ---
Performing Activate on Active/Standby

*Nov 20 21:45:21.695 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds  [R0] Activate package(s) on R0
  [R0] Finished Activate on R0
  [R1] Activate package(s) on R1
  [R1] Finished Activate on R1
Checking status of Activate on [R0 R1]
Activate: Passed on [R0 R1]
Finished Activate


*Nov 20 21:45:25.233 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R1/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds--- Starting Commit ---
Performing Commit on Active/Standby
  [R0] Commit package(s) on R0
  [R0] Finished Commit on R0
  [R1] Commit package(s) on R1
  [R1] Finished Commit on R1
Checking status of Commit on [R0 R1]
Commit: Passed on [R0 R1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Mon Nov 20 21:46:18 IST 2023
```

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 ROMMON version does not downgrade. It remains updated.

The following sample output of the **show version** command displays the Cisco IOS XE 17.13.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.13.01
Cisco IOS Software [Dublin], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.13.1,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2023 by Cisco Systems, Inc.
<output truncated>
```

Field-Programmable Gate Array Version Upgrade

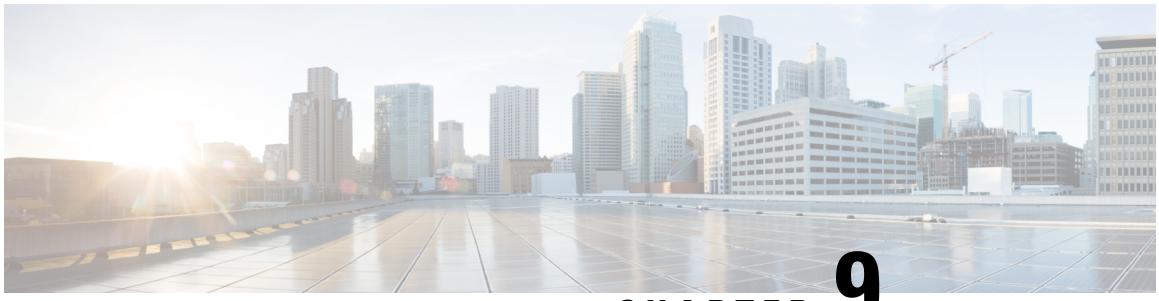
A field-programmable gate array (FPGA) is a type of programmable memory device that exists on Cisco switches. They are re-configurable logic circuits that enable the creation of specific and dedicated functions.

To check the current FPGA version, enter the **show firmware version all** command in privileged EXEC mode or the **version -v** command in ROMMON mode.



Note

- Not every software release has a change in the FPGA version.
- The version change occurs as part of the regular software upgrade and you do not have to perform any other additional steps.



CHAPTER 9

Caveats

- Cisco Bug Search Tool, on page 41
- Open Caveats in Cisco IOS XE 17.14.x, on page 41
- Resolved Caveats in Cisco IOS XE 17.14.1, on page 41

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.

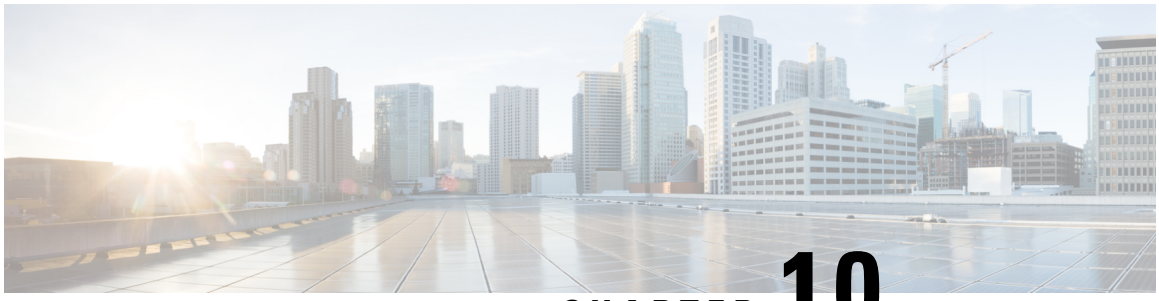
To view the details of a caveat, click on the identifier.

Open Caveats in Cisco IOS XE 17.14.x

Identifier	Headline
CSCvu14870	Cat9k / Archive command causing 'bulk sync failure' and reloading Standby
CSCwj38294	C9600X and C9500X is dropping IPv6 ND packets.
CSCwq83338	On the C9600 Dual-Sup, performing a redundancy force-switchover immediately after reaching STANDBY HOT causes the process to halt at "in progress to standby cold-config"

Resolved Caveats in Cisco IOS XE 17.14.1

Identifier	Headline
CSCwi04837	C9600-LC-48TX LED ON although no cable



CHAPTER 10

Additional Information

- Troubleshooting, on page 43
- Related Documentation, on page 43
- Communications, Services, and Additional Information, on page 43

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 9600 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9600-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 Marketplace.

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

Cisco Bug Search Tool

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

© 2024 Cisco Systems, Inc. All rights reserved.