Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Amsterdam 17.1.x

First Published: 2019-11-26

Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Amsterdam 17.1.x

Introduction

Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance are leading, fixed, core and aggregation enterprise switching platforms and have been purpose-built to address emerging trends in security, IoT, mobility, and cloud.

These switches deliver complete convergence in terms of ASIC architecture with Unified Access Data Plane (UADP) 2.0 on Cisco Catalyst 9500 Series Switches and UADP 3.0 on Cisco Catalyst 9500 Series Switches - High Performance. The platform runs an open Cisco IOS XE that supports model-driven programmability. This series forms the foundational building block for Software-Defined Access (SD-Access), which is Cisco's lead enterprise architecture.

Note With the introduction of the High Performance models in the series, there may be differences in the supported and unsupported features, limitations, and caveats that apply to the Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance models. Throughout this release notes document, any such differences are expressly called out. If they are not, the information applies to all the models in the series.

Whats New in Cisco IOS XE Amsterdam 17.1.1

Hardware Features in Cisco IOS XE Amsterdam 17.1.1

- Table 1: Hardware Features Introduced on Cisco Catalyst 9500 Series Switches (C9500-12Q, C9500-16X, C9500-24Q, C9500-40X)
- Table 2: Hardware Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance (C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C

Table 1: Hardware Features Introduced on Cisco Catalyst 9500 Series Switches (C9500-12Q, C9500-16X, C9500-24Q, C9500-40X)

Feature Name	Description and Documentation Link
Direct-Attach Cables for Cisco QSA Module CVR-QSFP-SFP10G	Supported cable product numbers: • SFP-H10GB-ACU7M, SFP-H10GB-ACU10M • SFP-H10GB-CU1M, SFP-H10GB-CU3M, SFP-H10GB-CU5M • SFP-10G-AOC1M, SFP-10G-AOC2M, SFP-10G-AOC3M, SFP-10G-AOC5M, SFP-10G-AOC7M, SFP-10G-AOC10M For information about these cables, see Cisco 10GBASE SFP+ Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Table 2: Hardware Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance (C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C

Feature Name	Description and Documentation Link

Direct-Attach Cables for Cisco QSFP to SFP or SFP+ Adapter (QSA) Module CVR-QSFP-SFP10G	• Supported cable product numbers
	  • SFP-H10GB-CU1-5M, SFP-H10GB-CU2M, SFP-H10GB-CU2-5M,
	  • SFP-H10GB-ACU7M, SFP-H10GB-ACU10M
	  • SFP-10G-AOC1M, SFP-10G-AOC2M, SFP-10G-AOC3M, SFP-10G-AOC5M, SFP-10G-AOC7M, SFP-10G-AOC10M
	• Compatible switch models—C9500-32C, C9500-32QC, C9500-48Y4C, C9500-24Y4C
	For information about these cables, see Cisco 10GBASE SFP+ Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Software Features in Cisco IOS XE Amsterdam 17.1.1

• Software Features Introduced on All Models, on page 2
• Software Features Introduced on Cisco Catalyst 9500 Series Switches, on page 5
• Software Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance, on page 6

Software Features Introduced on All Models

Feature Name	Description, Documentation Link, and License Level Information
ERSPAN IPv6	Introduces IPv6 support for Encapsulated Remote Switched Port Analyzer (ERSPAN). ERSPAN enables you to monitor traffic on ports or VLANs, and send the monitored traffic to destination ports. See Network Management → Configuring ERSPAN. (DNA Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Flash MIB instance retrieval count limit increase	The limitation of Flash MIB listing 100 files per partition per device has been removed. Flash MIB can now fetch all the files from the flash file system. See Network Management → Configuring Simple Network Management Protocol. (Network Essentials and Network Advantage)
IGMP (IPv4) : VPLS Layer 2 Snooping	Introduces support for Internet Group Management Protocol (IGMP) snooping on a Virtual Private LAN Service (VPLS) configured network. See Multiprotocol Label Switching → Configuring Virtual Private LAN Service (VPLS) and VPLS BGP-Based Autodiscovery. (Network Advantage)
Ingress and Egress Flexible Netflow on MPLS	Allows capture of IP flow information for packets undergoing Multiprotocol Label Switching (MPLS) label imposition when entering an MPLS network. These packets arrive on a device as IP packets and are transmitted as MPLS packets. Enable the feature by configuring an ingress flow monitor for IPv4 and IPv6 traffic at the customer edge (CE) facing side of the provider edge (PE) node. See Network Management → Configuring Flexible NetFlow. (DNA Essentials and DNA Advantage)
MACsec over Ethernet over MPLS (EoMPLS)	In VLAN mode, the switch (PE device) can now process packets in which the 802.1Q tag is not encrypted by the CE device. See Multiprotocol Label Switching → Configuring Ethernet-over-MPLS and Pseudowire Redundancy. (Network Advantage)
Multicast VPN Extranet Support	Enables service providers to distribute IP multicast content originating from one enterprise site to other enterprise sites. See IP Multicast Routing → Configuring Multicast VPN Extranet Support. (Network Advantage)
MPLS VPN InterAS Option A	MPLS VPN InterAS options provide multiple ways of interconnecting VPNs between different MPLS VPN service providers. With one of the options configured, a customer's site can exist on several carrier networks (autonomous systems) and still have seamless VPN connectivity. Of the available InterAS options, MPLS VPN InterAS Option A is the simplest to configure. This option provides back-to-back virtual routing and forwarding (VRF) connectivity (MPLS VPN providers exchange routes across VRF interfaces). See Multiprotocol Label Switching → Configuring MPLS VPN InterAS Options. (Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Neighbor Discovery (ND) Inspection Feature Deprecation	The IPv6 ND Inspection feature is deprecated. The Switch Integrated Security Features based (SISF-based) device tracking feature replaces it and offers the same capabilities. See Security → Configuring IPv6 First Hop Security. (Network Essentials and Network Advantage)
Programmability • Candidate Configuration Commit Confirm • Model-Driven Telemetry Event Notification Support • RESTCONF YANG-Patch Support • Python 3 Support in Guest Shell • TLS for gRPC Dial-Out • SGACL and Environment Data Download over REST	The following programmability features are introduced in this release: • The candidate configuration supports the confirmed commit capability. This implementation is as specified in RFC 6241 for the confirmed commit capability which, when issued, sets the running configuration to the current contents of the candidate configuration and starts a confirmed commit timer. The confirmed commit operation will be rolled back if the commit is not issued within the timeout period. The default timeout period is 600 seconds or 10 minutes. • Model-Driven Telemetry Event Notification Support: Introduces support for event notifications over the NETCONF protocol. • RESTCONF YANG-Patch Support: Introduces support for YANG-Patch media type as specified by RFC 8072. • Python 3 Support in Guest Shell: Introduces support for Python Version 3.6 is supported in Guest Shell. • TLS for gRPC Dial-Out: Introduces support for TLS for gRPC dial-out. • Cisco TrustSec uses the REST-based transport protocol for SGACL policy provisioning and data download from Cisco Identity Services Engine (ISE). The REST-based protocol is more secure, and provides reliable, and faster policy and environment data provisioning, than the RADIUS protocol that is used in previous releases. Both the REST API-based and RADIUS-based download of Cisco TrustSec data is supported. However, only one protocol can be active on a device. In Cisco IOS XE Amsterdam 17.1.1, REST-based protocol is the default. • 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/1711. Some of the models introduced in this release are not backward compatible. For the complete list, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1711/BIC. Revision statements embedded in the YANG files indicate if there has been a model revision. The *README.md* file in the same GitHub location highlights changes that have been made in the release. See Programmability. (Network Essentials and Network Advantage)
VPLS Flow-Aware Transport Pseudowire Support	Provides the capability to identify individual flows within a pseudowire (PW) and provides devices the ability to use these flows to load-balance traffic. See Multiprotocol Label Switching → Configuring Virtual Private LAN Service (VPLS) and VPLS BGP-Based Autodiscovery. (Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
VPLS Protocol-Mode CLI Support	Introduces support for VPLS and VPLS BGP-based Autodiscovery configurations using protocol-CLI mode. See Multiprotocol Label Switching → Configuring Virtual Private LAN Service (VPLS) and VPLS BGP-Based Autodiscovery. (Network Advantage)

New on the Web UI	
• New default credentials for WebUI • Power Over Ethernet (POE) • Intermediate System-Intermediate System(IS-IS) • Routing Information Protocol (RIP) • Virtual Terminal Lines (VTY)	Use the WebUI for: • New default credentials for WebUI—The login credentials for connecting to the device from the WebUI at Day 0 have been updated. This is available in the respective platform hardware guide. • Power Over Ethernet (POE)—The dashboard displays a dashlet for POE utilization for the switch. • Intermediate System- Intermediate System(IS-IS)—Supports Integrated Intermediate System-Intermediate System(IS-IS) routing protocol configuration for improved routing of data packets to their destination based on the best route. • Routing Information Protocol (RIP)—Supports RIP configuration for improved routing of data packets to their destination based on the hop count. • Virtual Terminal Lines (VTY)—Supports vty lines configuration in device setup, to allow a maximum number of simultaneous access to the device, remotely, through Telnet or SSH.

Software Features Introduced on Cisco Catalyst 9500 Series Switches

Feature Name	Description, Documentation Link, and License Level Information
BIOS Protection : Capsule Upgrade	Enables upgrade of golden ROMMON using the **upgrade rom-monitor capsule golden switch** command in privileged EXEC mode. See System Management → BIOS Protection. (Network Essentials and Network Advantage)
IGMP Proxy for multiple upstream interfaces	Enables you to send Protocol Independent Multicast (PIM) joins to multiple upstream devices. See IP Multicast Routing → Configuring IGMP Proxy. (Network Advantage)
Opening or Closing SNMP UDP Ports	A security enhancement that enables you to access the Simple Network Management Protocol (SNMP) UDP ports only after one of the requisite commands is configured. This design change secures and opens the ports only when required and prevents a device from listening to a port unnecessarily. See Network Management → Configuring Simple Network Management Protocol. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Per-Port MTU Configuration	Introduces support for port level and port channel level maximum transmission unit (MTU) configuration. With Per-Port MTU configuration, you can configure different MTU values for different interfaces as well as for different port channel interfaces. See Interface and Hardware Components → Configuring Per-Port MTU. (Network Essentials and Network Advantage)

Software Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance

Feature Name	Description, Documentation Link, and License Level Information
Bluetooth Dongle	Introduces support for external USB Bluetooth dongles. The connected dongle acts as a Bluetooth host and serves as a management port connection on the device. See Interface and Hardware Components → Configuring an External USB Bluetooth Dongle. (Network Essentials and Network Advantage)
Generic Routing Encapsulation (GRE) IPv6 Tunnels	Enables delivery of packets from other protocols through an IPv6 network and allows the routing of IPv6 packets between private networks across public networks with globally routed IPv6 addresses. See IP Addressing Services → Configuring GRE IPv6 Tunnels. (Network Essentials and Network Advantage)

Important Notes

- Cisco StackWise Virtual - Supported and Unsupported Features, on page 6
- Unsupported Features—All Models, on page 7
- Unsupported Features—Cisco Catalyst 9500 Series Switches, on page 7
- Unsupported Features—Cisco Catalyst 9500 Series Switches - High Performance, on page 7
- Complete List of Supported Features, on page 8
- Accessing Hidden Commands, on page 8
- Default Behaviour—All Models, on page 9
- Default Interface Behaviour on Cisco Catalyst 9500 Series Switches - High Performance Only, on page 9

Cisco StackWise Virtual - Supported and Unsupported Features

When you enable Cisco StackWise Virtual on the device

- Layer 2, Layer 3, Security, Quality of Service, Multicast, Application, Monitoring and Management, Multiprotocol Label Switching, High Availability, BGP EVPN VXLAN, Remote Switched Port Analyzer, and Sofware Defined Access are supported.

  Contact the Cisco Technical Support Centre for the specific list of features that are supported under each one of these technologies.

- Resilient Ethernet Protocol is *not* supported.

Unsupported Features—All Models

- IPsec VPN
- Performance Monitoring (PerfMon)
- Virtual Routing and Forwarding (VRF)-Aware web authentication

Unsupported Features—Cisco Catalyst 9500 Series Switches

- Border Gateway Protocol (BGP) Additional Paths
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Flexible NetFlow—NetFlow v5 Export Protocol, 4-byte (32-bit) AS Number Support, TrustSec NetFlow IPv4 Security Group Access Control List (SGACL) Deny and Drop Export
- Lawful Intercept (LI)
- PIM Bidirectional Forwarding Detection (PIM BFD), PIM Snooping.
- Quality of Service—Classification (Layer 3 Packet Length, Time-to-Live (TTL)), per queue policer support, sharped profile enablement for egress per port queues, L2 Miss, Ingress Packet FIFO (IPF)
- Unicast over Point to Multipoint (P2MP) Generic Routing Encapsulation (GRE), Multicast over P2MP GRE.
- VLAN Translation—One-to-One Mapping

Unsupported Features—Cisco Catalyst 9500 Series Switches - High Performance

- Cisco Application Visibility and Control (AVC)
- Flexlink+
- VLAN Load Balancing for FlexLink+
- Preemption for VLAN Load Balancing
- FlexLink+ Dummy Multicast Packets
- Next Generation Network-Based Application Recognition (NBAR) and Next Generation NBAR (NBAR2)
- MPLS Label Distribution Protocol (MPLS LDP) VRF-Aware Static Labels
- QoS Options on GRE Tunnel Interfaces

Complete List of Supported Features

For the complete list of features supported on a platform, see the Cisco Feature Navigator at https://www.cisco.com/go/cfn.

When you search for the list of supported features by platform, select

- CAT9500—to see all the features supported on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models
- CAT9500 HIGH PERFORMANCE (32C; 32QC; 48Y4C; 24Y4C)—to see all the features supported on the C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C models

Accessing Hidden Commands

Starting with Cisco IOS XE Fuji 16.8.1a, as an improved security measure, the way in which hidden commands can be accessed has changed.

Hidden commands have always been present in Cisco IOS XE, but not equipped with CLI help. This means that entering a question mark (?) at the system prompt does not display the list of available commands. These commands are only meant to assist Cisco TAC in advanced troubleshooting and are not documented either.

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. Entering enter a question mark (?) at the system prompt displays 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 the command is used. For example:

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

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



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

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

Default Behaviour—All Models

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).

Default Interface Behaviour on Cisco Catalyst 9500 Series Switches - High Performance Only

Starting with Cisco IOS XE Gibraltar 16.11.1, the default interface for all High Performance models in the series changes from Layer 3 to Layer 2. Use the **no switchport** command to change the Layer 2 interface into Layer 3 mode.

The startup configuration has explicit configuration of the **switchport** command for Layer 2 interfaces and the **no switchport** command for Layer 3 interfaces to address this change in behaviour and to support seamless migration.

Supported Hardware

Cisco Catalyst 9500 Series Switches—Model Numbers

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

Base PIDs are the model numbers of the switch.

Bundled PIDs indicate the orderable part numbers for base PIDs that are bundled with a particular network module. Entering the **show version**, **show module**, or **show inventory** commands on such a switch (bundled PID), displays its base PID.

Table 3: Cisco Catalyst 9500 Series Switches

Switch Model	Default License Level	Description
Base PIDs		
C9500-12Q-E	Network Essentials	12 40-Gigabit Ethernet QSFP+ ports and two power supply slots
C9500-12Q-A	Network Advantage	
C9500-16X-E	Network Essentials	16 1/10-Gigabit Ethernet SFP/SFP+ ports and two power supply slots
C9500-16X-A	Network Advantage	
C9500-24Q-E	Network Essentials	24-Port 40-Gigabit Ethernet QSFP+ ports and two power supply slots
C9500-24Q-A	Network Advantage	
C9500-40X-E	Network Essentials	40 1/10-Gigabit Ethernet SFP/SFP+ ports and two power supply slots
C9500-40X-A	Network Advantage	
Bundled PIDs		

Switch Model	Default License Level	Description
C9500-16X-2Q-E	Network Essentials	16 10-Gigabit Ethernet SFP+ port switch and a 2-Port 40-Gigabit Ethernet (QSFP) network module on uplink ports
C9500-16X-2Q-A	Network Advantage	
C9500-24X-E	Network Essentials	16 10-Gigabit Ethernet SFP+ port switch and an 8-Port 10-Gigabit Ethernet (SFP) network module on uplink ports
C9500-24X-A	Network Advantage	
C9500-40X-2Q-E	Network Essentials	40 10-Gigabit Ethernet SFP+ port switch and a 2-Port 40-Gigabit Ethernet (QSFP) network module on uplink ports
C9500-40X-2Q-A	Network Advantage	
C9500-48X-E	Network Essentials	40 10-Gigabit Ethernet SFP+ port switch and an 8-Port 10-Gigabit Ethernet (SFP) network module on uplink ports
C9500-48X-A	Network Advantage	

Table 4: Cisco Catalyst 9500 Series Switches-High Performance

Switch Model	Default License Level	Description
C9500-24Y4C-E	Network Essentials	24 SFP28 ports that support 1/10/25-GigabitEthernet connectivity, four QSFP uplink ports that support 100/40-GigabitEthernet connectivity; two power supply slots.
C9500-24Y4C-A	Network Advantage	
C9500-32C-E	Network Essentials	32 QSFP28 ports that support 40/100 GigabitEthernet connectivity; two power supply slots.
C9500-32C-A	Network Advantage	
C9500-32QC-E	Network Essentials	32 QSFP28 ports, where you can have 24 ports that support 40-GigabitEthernet connectivity and 4 ports that support 100-GigabitEthernet connectivity, OR 32 ports that support 40-GigabitEthernet connectivity, OR 16 ports that support 100-GigabitEthernet connectivity; two power supply slots.
C9500-32QC-A	Network Advantage	
C9500-48Y4C-E	Network Essentials	48 SFP28 ports that support 1/10/25-GigabitEthernet connectivity; four QSFP uplink ports that supports up to 100/40-GigabitEthernet connectivity; two power supply slots.
C9500-48Y4C-A	Network Advantage	

Network Modules

The following table lists optional network modules for uplink ports available with some configurations .

Network Module	Description
C9500-NM-8X	Cisco Catalyst 9500 Series Network Module 8-port 1/10 Gigabit Ethernet with SFP/SFP+ Note the supported switch models (Base PIDs): • C9500-40X • C9500-16X
C9500-NM-2Q	Cisco Catalyst 9500 Series Network Module 2-port 40 Gigabit Ethernet with QSFP+ Note the supported switch models (Base PIDs): • C9500-40X • C9500-16X

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

Compatibility Matrix

To view the software compatibility information between Cisco Catalyst 9500 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)

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 9500 Series Switches. 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 (C9500-12Q, C9500-24Q, C9500-16X, C9500-40X)	ROMMON Version (C9500-32C, C9500-32QC, C9500-24Y4C, C9500-48Y4C)	ROMMON Version (C9500X)
Amsterdam 17.1.1	17.1.1r [FC1]	17.1.1[FC1]	-

Upgrading the Switch Software

This section covers the various aspects of upgrading or downgrading the device software.

Note You cannot use the Web UI to install, upgrade, or downgrade device software.

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 Amsterdam 17.1.1	CAT9K_IOSXE	cat9k_iosxe.17.01.01.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.01.01.

Upgrading the ROMMON

To know the ROMMON or bootloader version that applies to every major and maintenance release, see ROMMON Versions, on page 12.

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

  On the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the series, *you must manually upgrade* the ROMMON in the primary SPI flash device, if a new version is applicable, and the release you are upgrading *from* is Cisco IOS XE Gibraltar 16.12.1 or a later release. (So if you upgrade from Cisco IOS XE Gibraltar 16.11.1 for example, a manual upgrade does not apply; the ROMMON is automatically updated, if applicable). Enter the **upgrade rom-monitor capsule primary switch** command in privileged EXEC mode.

  On the C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C models of the series, 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 when you boot up your switch with the new image for the first time.

- Upgrading the ROMMON in the golden SPI flash device

  You must manually upgrade this ROMMON. The manual upgrade applies to all models in the series. 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 switch.

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.

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.

There is no FPGA upgrade in Cisco IOS XE Amsterdam 17.1.1. To check the current FPGA version, enter 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.

Software Installation Commands

Summary of Software Installation Commands **Supported starting from Cisco IOS XE Everest 16.6.2 and later releases**	
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.

Note The **request platform software** commands are deprecated starting from Cisco IOS XE Gibraltar 16.10.1. The commands are visible on the CLI in this release and you can configure them, but we recommend that you use the **install** commands to upgrade or downgrade.

Summary of request platform software Commands **Note** **This table of commands is not supported on Cisco Catalyst 9500 Series Switches - High Performance.**	
`Device# request platform software package ?`	
clean	Cleans unnecessary package files from media
copy	Copies package to media
describe	Describes package content
expand	Expands all-in-one package to media
install	Installs the package
uninstall	Uninstalls the package
verify	Verifies In Service Software Upgrade (ISSU) software package compatibility

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 ...	Use these commands...	To upgrade to...
Cisco IOS XE Everest 16.5.1a or Cisco IOS XE Everest 16.6.1	Only **request platform software** commands	Cisco IOS XE Amsterdam 17.1.1
Cisco IOS XE Everest 16.6.2 and later	Either **install** commands or **request platform software** commands	

The sample output in this section displays upgrade from

- Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Amsterdam 17.1.1 using **request platform software** commands.
- Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Amsterdam 17.1.1 using **install** commands.

Procedure

Step 1 Clean Up

Ensure that you have at least 1GB of space in flash to expand a new image. Clean up old installation files in case of insufficient space.

- **request platform software package clean**
- **install remove inactive**

The following sample output displays the cleaning up of unused files, by using the **request platform software package clean** command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Amsterdam 17.1.1.

```
Switch# request platform software package clean switch all
Running command on switch 1
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-cc_srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.
done.

Running command on switch 2
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-cc_srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.SPA.pkg
```

```
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.

Running command on switch 3
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 ...
hexdump: NVRAM: No such file or directory
hexdump: all input file arguments failed
head: cannot open 'NVRAM' for reading: No such file or directory
NVRAM: No such file or directory
hexdump: NVRAM: No such file or directory
hexdump: stdin: Bad file descriptor
tail: cannot open 'NVRAM' for reading: No such file or directory
hexdump: NVRAM: No such file or directory
hexdump: all input file arguments failed
cat9k-cc_srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.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:
[1]:
/flash/cat9k-cc_srdriver.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-
[2]:
/flash/cat9k-cc_srdriver.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
```

```
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-
[3]:
/flash/cat9k-cc_srdriver.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-

Do you want to proceed? [y/n]y
[1]:
Deleting file flash:cat9k-cc_srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-webui.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[2]:
Deleting file flash:cat9k-cc_srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-webui.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[3]:
Deleting file flash:cat9k-cc_srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-webui.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted
```

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command, for upgrade scenario Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Amsterdam 17.1.1:

```
Switch# install remove inactive
install_remove: START Wed Nov 20 19:51:48 UTC 2019
```

```
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.
The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.16.12.01.SPA.pkg
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-guestshell.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
/flash/cat9k-webui.16.12.01.SPA.pkg
/flash/cat9k-wlc.16.12.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.12.01.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 Thu Nov 20 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

Use this command to copy the new image to flash: (or skip this step if you want to use the new image from your TFTP server)

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.17.01.01.SPA.bin flash:
destination filename [cat9k_iosxe.17.01.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.17.01.01.SPA.bin...
Loading /cat9k_iosxe.17.01.01.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 Nov 20 2019 10:18:11 -07:00 cat9k_iosxe.17.01.01.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
Switch(config)# exit
```

b) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

c) **show boot system**

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

The output should display **BOOT variable** = **flash:packages.conf**.

```
Switch# show boot system
```

Step 4 Software install image to flash

- **request platform software package install**
- **install add file activate commit**

You can point to the source image on your TFTP server or in flash if you have it copied to flash. We recommend copying the image to a TFTP server or the flash drive of the active switch. If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For example, if the image is on the flash drive of member switch 3 (flash-3):

`Switch# request platform software package install switch all file flash-3:cat9k_iosxe.17.01.01.SPA.bin auto-copy`.

The following sample output displays installation of the Cisco IOS XE Amsterdam 17.1.1 software image to flash, by using the **request platform software package install** command, for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Amsterdam 17.1.1.

```
Switch# request platform software package install switch all file
flash:cat9k_iosxe.17.01.01.SPA.bin auto-copy

--- Starting install local lock acquisition on switch 1 ---
Finished install local lock acquisition on switch 1

Expanding image file: flash:cat9k_iosxe.17.01.01.SPA.bin
[1]: Copying flash:cat9k_iosxe.17.01.01.SPA.bin from switch 1 to switch 2 3
[2 3]: Finished copying to switch 2 3
[1 2 3]: Expanding file
[1 2 3]: Finished expanding all-in-one software package in switch 1 2 3
SUCCESS: Finished expanding all-in-one software package.
[1 2 3]: Performing install
SUCCESS: install finished
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
```

```
Old files list:
Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
Removed cat9k-sipbase.16.05.01a.SPA.pkg
Removed cat9k-sipspa.16.05.01a.SPA.pkg
Removed cat9k-srdriver.16.05.01a.SPA.pkg
Removed cat9k-webui.16.05.01a.SPA.pkg
Removed cat9k-wlc.16.05.01a.SPA.pkg
New files list:
Added cat9k-cc_srdriver.17.01.01.SPA.pkg
Added cat9k-espbase.17.01.01.SPA.pkg
Added cat9k-guestshell.17.01.01.SPA.pkg
Added cat9k-rpbase.17.01.01.SPA.pkg
Added cat9k-rpboot.17.01.01.SPA.pkg
Added cat9k-sipbase.17.01.01.SPA.pkg
Added cat9k-sipspa.17.01.01.SPA.pkg
Added cat9k-srdriver.17.01.01.SPA.pkg
Added cat9k-webui.17.01.01.SPA.pkg
Added cat9k-wlc.17.01.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[1]: Finished install successful on switch 1
[2]: install package(s) on switch 2
--- Starting list of software package changes ---
Old files list:
Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
Removed cat9k-sipbase.16.05.01a.SPA.pkg
Removed cat9k-sipspa.16.05.01a.SPA.pkg
Removed cat9k-srdriver.16.05.01a.SPA.pkg
Removed cat9k-webui.16.05.01a.SPA.pkg
Removed cat9k-wlc.16.05.01a.SPA.pkg
New files list:
Added cat9k-cc_srdriver.17.01.01.SPA.pkg
Added cat9k-espbase.17.01.01.SPA.pkg
Added cat9k-guestshell.17.01.01.SPA.pkg
Added cat9k-rpbase.17.01.01.SPA.pkg
Added cat9k-rpboot.17.01.01.SPA.pkg
Added cat9k-sipbase.17.01.01.SPA.pkg
Added cat9k-sipspa.17.01.01.SPA.pkg
Added cat9k-srdriver.17.01.01.SPA.pkg
Added cat9k-webui.17.01.01.SPA.pkg
Added cat9k-wlc.17.01.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[2]: Finished install successful on switch 2
[3]: install package(s) on switch 3
--- Starting list of software package changes ---
Old files list:
Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
Removed cat9k-sipbase.16.05.01a.SPA.pkg
Removed cat9k-sipspa.16.05.01a.SPA.pkg
Removed cat9k-srdriver.16.05.01a.SPA.pkg
Removed cat9k-webui.16.05.01a.SPA.pkg
```

```
Removed cat9k-wlc.16.05.01a.SPA.pkg
New files list:
Added cat9k-cc_srdriver.17.01.01.SPA.pkg
Added cat9k-espbase.17.01.01.SPA.pkg
Added cat9k-guestshell.17.01.01.SPA.pkg
Added cat9k-rpbase.17.01.01.SPA.pkg
Added cat9k-rpboot.17.01.01.SPA.pkg
Added cat9k-sipbase.17.01.01.SPA.pkg
Added cat9k-sipspa.17.01.01.SPA.pkg
Added cat9k-srdriver.17.01.01.SPA.pkg
Added cat9k-webui.17.01.01.SPA.pkg
Added cat9k-wlc.17.01.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[3]: Finished install successful on switch 3
Checking status of install on [1 2 3]
[1 2 3]: Finished install in switch 1 2 3
SUCCESS: Finished install: Success on [1 2 3]
```

Note
Old files listed in the logs are not removed from flash.

The following sample output displays installation of the Cisco IOS XE Amsterdam 17.1.1 software image to flash, by using the **install add file activate commit** command, for upgrade scenario Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Amsterdam 17.1.1:

```
Switch# install add file flash:cat9k_iosxe.17.01.01.SPA.bin activate commit

install_add_activate_commit: START Thu Nov 20 19:54:51 UTC 2018

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]y
Building configuration...

[OK]Modified configuration has been saved

*Nov 20 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Nov 20 19:54:55 install_engine.sh:

%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.17.01.01.SPA.bininstall_add_activate_commit: Adding PACKAGE

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 ---
Info: Finished copying flash:cat9k_iosxe.17.01.01.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

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.01.01.SPA.pkg
/flash/cat9k-webui.17.01.01.SPA.pkg
/flash/cat9k-srdriver.17.01.01.SPA.pkg
```

```
/flash/cat9k-sipspa.17.01.01.SPA.pkg
/flash/cat9k-sipbase.17.01.01.SPA.pkg
/flash/cat9k-rpboot.17.01.01.SPA.pkg
/flash/cat9k-rpbase.17.01.01.SPA.pkg
/flash/cat9k-guestshell.17.01.01.SPA.pkg
/flash/cat9k-espbase.17.01.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.01.01.SPA.pkg

This operation requires a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on all members
[1] Activate package(s) on switch 1
[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

*Nov 20 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: nov 20 19:57:41 rollback_timer.sh:

%INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Install auto abort timer will expire in 7200
 seconds [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 Thu Nov 20 19:57:48 UTC 2019
Switch#
```

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 **dir flash:**

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

The following is sample output of the **dir flash:** command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Amsterdam 17.1.1:

```
Switch# dir flash:*.pkg

Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104   Jul 26 2017 09:52:41 -07:00 cat9k-cc_srdriver.16.05.01a.SPA.pkg
475141 -rw- 70333380  Jul 26 2017 09:52:44 -07:00 cat9k-espbase.16.05.01a.SPA.pkg
475142 -rw- 13256     Jul 26 2017 09:52:44 -07:00 cat9k-guestshell.16.05.01a.SPA.pkg
475143 -rw- 349635524 Jul 26 2017 09:52:54 -07:00 cat9k-rpbase.16.05.01a.SPA.pkg
475149 -rw- 24248187  Jul 26 2017 09:53:02 -07:00 cat9k-rpboot.16.05.01a.SPA.pkg
475144 -rw- 25285572  Jul 26 2017 09:52:55 -07:00 cat9k-sipbase.16.05.01a.SPA.pkg
475145 -rw- 20947908  Jul 26 2017 09:52:55 -07:00 cat9k-sipspa.16.05.01a.SPA.pkg
475146 -rw- 2962372   Jul 26 2017 09:52:56 -07:00 cat9k-srdriver.16.05.01a.SPA.pkg
475147 -rw- 13284288  Jul 26 2017 09:52:56 -07:00 cat9k-webui.16.05.01a.SPA.pkg
475148 -rw- 13248     Jul 26 2017 09:52:56 -07:00 cat9k-wlc.16.05.01a.SPA.pkg

491524 -rw- 25711568  Nov 20 2019 11:49:33 -07:00 cat9k-cc_srdriver.17.01.01.SPA.pkg
491525 -rw- 78484428  Nov 20 2019 11:49:35 -07:00 cat9k-espbase.17.01.01.SPA.pkg
```

```
491526 -rw- 1598412   Nov 20 2019 11:49:35 -07:00 cat9k-guestshell.17.01.01.SPA.pkg
491527 -rw- 404153288 Nov 20 2019 11:49:47 -07:00 cat9k-rpbase.17.01.01.SPA.pkg
491533 -rw- 31657374  Nov 20 2019 11:50:09 -07:00 cat9k-rpboot.17.01.01.SPA.pkg
491528 -rw- 27681740  Nov 20 2019 11:49:48 -07:00 cat9k-sipbase.17.01.01.SPA.pkg
491529 -rw- 52224968  Nov 20 2019 11:49:49 -07:00 cat9k-sipspa.17.01.01.SPA.pkg
491530 -rw- 31130572  Nov 20 2019 11:49:50 -07:00 cat9k-srdriver.17.01.01.SPA.pkg
491531 -rw- 14783432  Nov 20 2019 11:49:51 -07:00 cat9k-webui.17.01.01.SPA.pkg
491532 -rw- 9160      Nov 20 2019 11:49:51 -07:00 cat9k-wlc.17.01.01.SPA.pkg

11353194496 bytes total (8963174400 bytes free)
```

The following is sample output of the **dir flash:** command for the Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Amsterdam 17.1.1 upgrade scenario:

```
Switch# dir flash:*.pkg

Directory of flash:/
475140 -rw- 2012104   Jul 26 2019 09:52:41 -07:00 cat9k-cc_srdriver.16.12.01.SPA.pkg
475141 -rw- 70333380  Jul 26 2019 09:52:44 -07:00 cat9k-espbase.16.12.01.SPA.pkg
475142 -rw- 13256     Jul 26 2019 09:52:44 -07:00 cat9k-guestshell.16.12.01.SPA.pkg
475143 -rw- 349635524 Jul 26 2019 09:52:54 -07:00 cat9k-rpbase.16.12.01.SPA.pkg
475149 -rw- 24248187  Jul 26 2019 09:53:02 -07:00 cat9k-rpboot.16.12.01.SPA.pkg
475144 -rw- 25285572  Jul 26 2019 09:52:55 -07:00 cat9k-sipbase.16.12.01.SPA.pkg
475145 -rw- 20947908  Jul 26 2019 09:52:55 -07:00 cat9k-sipspa.16.12.01.SPA.pkg
475146 -rw- 2962372   Jul 26 2019 09:52:56 -07:00 cat9k-srdriver.16.12.01.SPA.pkg
475147 -rw- 13284288  Jul 26 2019 09:52:56 -07:00 cat9k-webui.16.12.01.SPA.pkg
475148 -rw- 13248     Jul 26 2019 09:52:56 -07:00 cat9k-wlc.16.12.01.SPA.pkg

491524 -rw- 25711568  Nov 20 2019 11:49:33 -07:00 cat9k-cc_srdriver.17.01.01.SPA.pkg
491525 -rw- 78484428  Nov 20 2019 11:49:35 -07:00 cat9k-espbase.17.01.01.SPA.pkg
491526 -rw- 1598412   Nov 20 2019 11:49:35 -07:00 cat9k-guestshell.17.01.01.SPA.pkg
491527 -rw- 404153288 Nov 20 2019 11:49:47 -07:00 cat9k-rpbase.17.01.01.SPA.pkg
491533 -rw- 31657374  Nov 20 2019 11:50:09 -07:00 cat9k-rpboot.17.01.01.SPA.pkg
491528 -rw- 27681740  Nov 20 2019 11:49:48 -07:00 cat9k-sipbase.17.01.01.SPA.pkg
491529 -rw- 52224968  Nov 20 2019 11:49:49 -07:00 cat9k-sipspa.17.01.01.SPA.pkg
491530 -rw- 31130572  Nov 20 2019 11:49:50 -07:00 cat9k-srdriver.17.01.01.SPA.pkg
491531 -rw- 14783432  Nov 20 2019 11:49:51 -07:00 cat9k-webui.17.01.01.SPA.pkg
491532 -rw- 9160      Nov 20 2019 11:49:51 -07:00 cat9k-wlc.17.01.01.SPA.pkg
11353194496 bytes total (9544245248 bytes free)
Switch#
```

The following sample output 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.17.01.01.SPA.conf`— a backup copy of the newly installed packages.conf file

```
Switch# dir flash:*.conf

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

434197 -rw- 7406 Nov 20 2019 10:59:16 -07:00 packages.conf
516098 -rw- 7406 Nov 20 2019 10:58:08 -07:00 cat9k_iosxe.17.01.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

Step 6 Upgrade the ROMMON

- **upgrade rom-monitor capsule golden switch** (Applies to all models in the series)
- **upgrade rom-monitor capsule primary switch** (Applies only to the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models in the series)

Use this command to upgrade the ROMMON version. On the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models, configure both commands.

For more information about this, see Upgrading the ROMMON, on page 13 in this document.

After you enter the command, confirm upgrade at the system prompt.

```
Switch# upgrade rom-monitor capsule golden switch active R0
This operation will reload the switch and take a few minutes to complete. Do you want to
proceed (y/n)? [confirm]y
Switch#
Initializing Hardware...
<output truncated>
```

Step 7 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

If your switches are configured with auto boot, then the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
Switch: boot flash:packages.conf
```

c) **show version**

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

Note
When you boot the new image, the boot loader is automatically updated, but the new bootloader version is not displayed in the output until the next reload.

The following sample output of the **show version** command displays the Cisco IOS XE Gibraltar 16.12.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.01.01
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.1.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Wed 20-Nov-19 10:39 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 ...	Use these commands...	To downgrade to...
Cisco IOS XE Amsterdam 17.1.1	• On Cisco Catalyst 9500 Series Switches, either **install** commands or **request platform software** commands • On Cisco Catalyst 9500 Series Switches - High Performance, **install** commands	Cisco IOS XE Gibraltar 16.12.x or earlier releases

On Cisco Catalyst 9500 Series Switches - High Performance, **install** commands

Procedure

Step 1 Clean Up

Ensure that you have at least 1GB of space in flash to expand a new image. Clean up old installation files in case of insufficient space.

- **request platform software package clean**
- **install remove inactive**

The following sample output displays the cleaning up of Cisco IOS XE Amsterdam 17.1.1 files using the **install remove inactive** command:

```
Switch# install remove inactive

install_remove: START Wed Nov 20 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.17.01.01.SPA.pkg
/flash/cat9k-espbase.17.01.01.SPA.pkg
/flash/cat9k-guestshell.17.01.01.SPA.pkg
/flash/cat9k-rpbase.17.01.01.SPA.pkg
/flash/cat9k-rpboot.17.01.01.SPA.pkg
/flash/cat9k-sipbase.17.01.01.SPA.pkg
/flash/cat9k-sipspa.17.01.01.SPA.pkg
/flash/cat9k-srdriver.17.01.01.SPA.pkg
/flash/cat9k-webui.17.01.01.SPA.pkg
/flash/cat9k-wlc.17.01.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.17.01.01.SPA.pkg ... done.
```

```
Deleting file flash:cat9k-srdriver.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.17.01.01.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 Wed Nov 20 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

Use this command to copy the new image to flash: (or skip this step if you want to use the new image from your TFTP server)

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.12.01.SPA.bin flash:
Destination filename [cat9k_iosxe.16.12.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.12.01.SPA.bin...
Loading /cat9k_iosxe.16.12.01.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 Jul 22 2018 13:35:16 -07:00 cat9k_iosxe.16.12.01.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Downgrade software image

- **install add file activate commit**
- **request platform software package install**

The following example displays the installation of the Cisco IOS XE Gibraltar 16.12.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.16.12.01.SPA.bin activate commit

install_add_activate_commit: START Mon Jul 22 19:54:51 UTC 2019

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]yBuilding
 configuration...
```

```
[OK]Modified configuration has been saved

*Jul 22 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 22 19:54:55 install_engine.sh:
 %INSTALL-
5-INSTALL_START_INFO: Started install one-shot flash:cat9k_iosxe.16.12.01.SPA.bin
install_add_activate_commit: Adding PACKAGE

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 ---
Info: Finished copying flash:cat9k_iosxe.16.12.01.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

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.16.12.01.SPA.pkg
/flash/cat9k-webui.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-guestshell.16.12.01.SPA.pkg
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.12.01.SPA.pkg

This operation requires a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on all members
[1] Activate package(s) on switch 1
[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

*Jul 22 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 22 19:57:41 rollback_timer.sh:
 %INSTALL-
5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Install auto abort timer will expire in 7200 seconds
[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 22 19:57:48 UTC 2019
Switch#
```

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

Step 4 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

If your switches are configured with auto boot, then the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
Switch: boot flash:packages.conf
```

Note
When you downgrade the software image, the boot loader will not automatically downgrade. It will remain updated.

c) **show version**

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

Note
When you boot the new image, the boot loader is automatically updated, but the new bootloader version is not displayed in the output until the next reload.

The following sample output of the **show version** command displays the Cisco IOS XE Gibraltar 16.12.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.12.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.12.1, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 20-Nov-19 19:26 by mcpre
<output truncated>
```

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 16.8.x and earlier: RTU Licensing is the default and the only supported method to manage licenses.
- Cisco IOS XE Fuji 16.9.1 to Cisco IOS XE Amsterdam 17.3.1: Smart Licensing is the default and the only supported method to manage licenses.

Note On the Cisco Catalyst 9500 Series Switches-High Performance, it is from Cisco IOS XE Fuji 16.8.1a to Cisco IOS XE Amsterdam 17.3.1.

- 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 9500 Series Switches datasheet at:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/datasheet-c78-738978.html

Limitations and Restrictions

With Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance—If a feature is not supported on a switch model, you do not have to factor in any limitations or restrictons that may be listed here. If limitations or restrictions are listed for a feature that is supported, check if model numbers are specified, to know if they apply. If model numbers are not specified, the limitations or restrictons apply to all models in the series.

- Auto negotiation

  Auto negotiation (the **speed auto** command) and half duplex (the **duplex half** command) are not supported on GLC-T or GLC-TE transceivers for 10 Mbps and 100 Mbps speeds. This applies only to the C9500-48Y4C and C9500-24Y4C models of the series.

  We recommend not changing Forward Error Correction (FEC) when auto negotiation is ON. This is applicable to 100G/40G/25G CU cables on the C9500-32C, C9500-32QC, C9500-24Y4C and C9500-48Y4C models of the series.

- 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.

- Cisco StackWise Virtual

  - On Cisco Catalyst 9500 Series Switches, when Cisco StackWise Virtual is configured, breakout ports using 4X10G breakout cables, or the Cisco QSFP to SFP or SFP+ Adapter (QSA) module can only be used as data ports; they cannot be used to configure StackWise Virtual links (SVLs) or dual-active detective (DAD) links.

  - On Cisco Catalyst 9500 Series Switches - High Performance,

    - When Cisco StackWise Virtual is configured, breakout ports using 4X25G or 4X10G breakout cables can only be used as data ports; they cannot be used to configure SVLs or DAD links.

    - When Cisco StackWise Virtual is configured, Cisco QSA module with 10G SFP modules can be used as data ports and to configure SVLs or DAD links.

- When Cisco StackWise Virtual is configured, Cisco QSA module with 1G SFP modules can be used as data ports and to configure DAD links; they cannot be used to configure SVLs since SVLs are not supported on 1G interfaces.

- Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
- Flexible NetFlow limitations
  - You cannot configure NetFlow export using the Ethernet Management port (GigabitEthernet0/0).
  - You can not configure a flow monitor on logical interfaces, such as layer 2 port-channels, loopback, tunnels.
  - You can not configure multiple flow monitors of same type (ipv4, ipv6 or datalink) on the same interface for same direction.
- Hardware limitations:
  - Use the MODE button to switch-off the beacon LED.
  - All port LED behavior is undefined until interfaces are fully initialized.
  - 1G with Cisco QSA Module (CVR-QSFP-SFP10G) is not supported on the uplink ports of the C9500-24Y4C and C9500-48Y4C models.
  - The following limitations apply to Cisco QSA Module (CVR-QSFP-SFP10G) when Cisco 1000Base-T Copper SFP (GLC-T) or Cisco 1G Fiber SFP Module for Multimode Fiber are plugged into the QSA module:
    - 1G Fiber modules over QSA do not support autonegotiation. Auto-negotiation should be disabled on the far-end devices.
    - Although visible in the CLI, the command [**no**] **speed nonegotiate** is not supported with 1G Fiber modules over QSA.
    - Only GLC-T over QSA supports auto-negotiation.
    - GLC-T supports only port speed of 1000 Mb/s over QSA. Port speeds of 10/100-Mb/s are not supported due to hardware limitation.
  - When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, autonegotiation is enabled by default. If the other end of the line does not support autonegotation, the link does not come up.
  - Autonegotiation is not supported on HundredGigabitEthernet1/0/49 to HundredGigabitEthernet1/0/52 uplink ports of the C9500-48Y4C models, and HundredGigabitEthernet1/0/25 to HundredGigabitEthernet1/0/28 uplink ports of the C9500-24Y4C models. Disable autonegotiation on the peer device if you are using QSFP-H40G-CUxx and QSFP-H40G-ACUxx cables.
  - For QSFP-H100G-CUxx cables, the C9500-48Y4C and C9500-24Y4C models support the cables only if both sides of the connection are either C9500-48Y4C or C9500-24Y4C.
- Interoperability limitations—When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, if one end of the 40G link is a Catalyst 9400 Series Switch and the other end is a Catalyst 9500 Series Switch, the link does not come up, or comes up on one side and stays down on the other. To avoid this

interoperability issue between devices, apply the the **speed nonegotiate** command on the Catalyst 9500 Series Switch interface. This command disables autonegotiation and brings the link up. To restore autonegotiation, use the **no speed nonegotiation** command.

- In-Service Software Upgrade (ISSU)
  - In-Service Software Upgrade (ISSU)—On Cisco Catalyst 9500 Series Switches (C9500-12Q, C9500-16X, C9500-24Q, C9500-40X), ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.10.x or to Cisco IOS XE Gibraltar 16.11.x is not supported.
  - On Cisco Catalyst 9500 Series Switches - High Performance (C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C), ISSU with Cisco StackWise Virtual is supported only starting from Cisco IOS XE Gibraltar 16.12.1. Therefore, ISSU upgrades can be performed only starting from this release to a later release.
  - 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%.
  - For QoS policies, only switched virtual interfaces (SVI) are supported for logical interfaces.
  - 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.

- 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
```

- 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.
- Wired Application Visibility and Control limitations:
  - NBAR2 (QoS and Protocol-discovery) configuration is allowed only on wired physical ports. It is not supported on virtual interfaces, for example, VLAN, port channel nor other logical interfaces.
  - NBAR2 based match criteria 'match protocol' is allowed only with marking or policing actions. NBAR2 match criteria will not be allowed in a policy that has queuing features configured.
  - 'Match Protocol': up to 256 concurrent different protocols in all policies.
  - NBAR2 and Legacy NetFlow cannot be configured together at the same time on the same interface. However, NBAR2 and wired AVC Flexible NetFlow can be configured together on the same interface.
  - Only IPv4 unicast (TCP/UDP) is supported.
  - AVC is not supported on management port (Gig 0/0)
  - NBAR2 attachment should be done only on physical access ports. Uplink can be attached as long as it is a single uplink and is not part of a port channel.
  - Performance—Each switch member is able to handle 500 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.
  - Scale—Able to handle up to 5000 bi-directional flows per 24 access ports and 10000 bi-directional flows per 48 access ports.
- 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.
- The File System Check (fsck) utility is not supported in install mode.
- 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.

Caveats

Caveats describe unexpected behavior in Cisco IOS-XE releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

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 Amsterdam 17.1.x

Identifier	Applicable models	Description
CSCvq72472	All models	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvr88090	All models	Cat9300 crash on running show platform software fed switch 1 fss abstraction
CSCvr90477	All models	9500 incorrectly set more-fragment flag for double fragmentation
CSCvr92287	All models	EPC with packet-len opt breaks CPU in-band path for bigger frames
CSCvr92660	All models	STP BPDUs not being sent from FED to IOSd
CSCvr98281	All models	After valid ip conflict, SVI admin down responds to GARP
CSCvr99132	All models	SPANed multicast packet reduced TTL
CSCvs14893	All models	802.1x-MultiAuth/MultiDomain: C9K - Traffic drop in egress direction for Data-Vlan on a Auth port
CSCvr68056	Catalyst 9500 High Performance	Link flap causes negotiation fail of flowcontrol
CSCvr96863	Catalyst 9500 High Performance	C9500-24Q QSFP interfaces on standby switch of stackwise virtual pair may remain down/down

Resolved Caveats in Cisco IOS XE Amsterdam 17.1.1

Identifier	Applicable Models	Description
CSCvo66246	All models	Enabling SPAN source of VLAN 1 affects LACP operations
CSCvp84502	All models	ERSPAN destination does not work or forward traffic
CSCvq05337	All models	Cat9500 || v169_3_hemit_es_throttle ES image || EGR_INVALID_REWRITE counter increasing in mVPN setup
CSCvq22224	All models	cat9k // evpn/vxlan // dhcp relay not working over l3vni
CSCvq29115	All models	Failed to get Board ID shown if stack member boots up
CSCvq30460	All models	SYS-2-BADSHARE: Bad refcount in datagram_done - messages seen during system churn
CSCvq40137	All models	Mac address not being learnt when "auth port-control auto" command is present

Identifier	Applicable Models	Description
CSCvq72713	All models	Cat3k/Cat9k can't forwarding traffic follow the rule of EIGRP unequal cost load-balancing
CSCvr04551	All models	Multicast stream flickers on igmp join/leave
CSCvr07162	All models	system crash on execute "fed TCAM utilization"
CSCvr46931	All models	ports remain down/down object-manager (fed-ots-mo thread is stuck)
CSCvq13053	Catalyst 9500	NAT translation entry not cleared after fin-rst time-out
CSCvq58991	Catalyst 9500	C9400/16.11.1 - Diagnostic test of TestPortTxMonitoring is failing for DAD links
CSCvq72181	Catalyst 9500	16.12.1 - Seeing 100% CPU with FED on 9500 SVL setup
CSCvp71508	Catalyst 9500 High Performance	Cat9500HP has same mac-address on mgmt port and first asic port after reload
CSCvq32597	Catalyst 9500 High Performance	C9500 High Performance - Port LED status not displayed correctly
CSCvq86372	Catalyst 9500 High Performance	Standby switch crashed on collecting temperature sensor information in obfl
CSCvq93773	Catalyst 9500 High Performance	C9600/9400/9500H/9300 etc crashes due to CMCC heartbeat failures
CSCvr55472	Catalyst 9500 High Performace	Breakout multiple interfaces via SNMP walk

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 9500 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9500-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)

© 2019 Cisco Systems, Inc. All rights reserved.