Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Amsterdam 17.1.x

First Published: 2019-11-26

Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Amsterdam 17.1.x

Introduction

Cisco Catalyst 9600 Series Switches are the next generation purpose-built 40 GigabitEthernet and 100 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 complete convergence in terms of ASIC architecture with Unified Access Data Plane (UADP) 3.0. 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.

Whats New in Cisco IOS XE Amsterdam 17.1.1

Hardware Features in Cisco IOS XE Amsterdam 17.1.1

Feature Name	Description and Documentation Link
C9600-LC-48TX	Cisco Catalyst 9600 Series 48-port supporting 10 G, 5 G, 2.5 G, 1 G, 100 Mbps and 10 Mbps on each of its 48 RJ45 ports. See Cisco Catalyst 9600 Series Line Card Installation Note.
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 For information about a cable, 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

Feature Name	Description, Documentation Link, and License Level Information
BIOS Protection for Golden SPI	Enables write-protection of the golden ROMMON image. See System Management → BIOS Protection. (Network Advanatge)
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 Advantage)
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)
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 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 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 Advantage)

Feature Name	Description, Documentation Link, and License Level Information
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)
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)
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)
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 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 Advantage)
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 Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Programmability	The following programmability features are introduced in this release: • 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 Advantage)
VPLS Flow-Aware Transport Pseudowire Support	Provides the capability to identify individual flows within a pseudowire 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)
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)
VPN Routing and Forwarding-aware Policy Based Routing (VRF-aware PBR)	The PBR feature is now VRF-aware and can be configured on VRF lite interfaces. You can enable policy based routing of packets for a VRF instance. See IP Routing → Configuring VRF aware PBR. (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.

Important Notes

Unsupported Features

- Breakout Cables
- Cisco Application Visibility and Control (AVC)
- IPsec VPN
- Network-Based Application Recognition (NBAR) and Next Generation NBAR (NBAR2)

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.

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. Hidden commands are 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

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).

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.
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
40 or 100 GigabitEthernet Line Cards	
C9600-LC-24C	Cisco Catalyst 9600 Series 24-Port 40GE/12-Port 100GE Line Card. It supports: • 12 ports of 100 GigabitEthernet (GE) or 24 ports of 40GE • QSFP on all ports and QSFP28 on the 100 GE ports
25 GigabitEthernet Line Cards	
C9600-LC-48YL	Cisco Catalyst 9600 Series 48-Port 25GE/10GE/1GE line card. It supports: • 48 ports of 25 GE, 10GE or 1GE • SFP28, SFP+ transceivers on all ports
10 GigabitEthernet Line Cards	

Product ID (append with "=" for spares)	Description
C9600-LC-48TX	Cisco Catalyst 9600 Series 48-port of 10GE/5GE/2.5GE/1GE/100Mbps/10 Mbps line card. • Provides 48 10 G, 5 G, 2.5 G, 1 G, 100 Mbps and 10Mbps interfaces by default. These ports can be interchangeably used as 10 G, 5 G, 2.5 G, 1 G, 100 Mbps and 10 Mbps ports. • All the 48 ports support 10 G, 5 G, 2.5 G, 1 G, 100 Mbps and 10 Mbps speeds.
AC Power Supply Modules	
C9600-PWR-2KWAC	Cisco Catalyst 9600 Series 2000W AC Power Supply Module[3]
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

Compatibility Matrix

The following table provides software compatibility information between Cisco Catalyst 9600 Series Switches, Cisco Identity Services Engine, Cisco Access Control Server, and Cisco Prime Infrastructure.

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Amsterdam 17.1.1	2.7	-	-
Gibraltar 16.12.8	2.6	-	-
Gibraltar 16.12.7	2.6	-	-
Gibraltar 16.12.6	2.6	-	-
Gibraltar 16.12.5b	2.6	-	-
Gibraltar 16.12.5	2.6	-	-

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.12.4	2.6	-	-
Gibraltar 16.12.3a	2.6	-	-
Gibraltar 16.12.3	2.6	-	-
Gibraltar 16.12.2	2.6	-	-
Gibraltar 16.12.1	2.6	-	-
Gibraltar 16.11.1	2.6 2.4 Patch 5	5.4 5.5	-

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)

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)
Amsterdam 17.1.1	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 10.

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 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. 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.

In case of a High Availability set up, 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 **show firmware version all** command in IOS 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.

Software Installation Commands

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

Upgrading in Install Mode

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

Before you begin

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 Gibraltar 16.12.1	Cisco IOS XE Amsterdam 17.1.1

The sample output in this section displays upgrade from Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Amsterdam 17.1.1 using **install** commands.

Procedure

Step 1 Clean Up

a) **install remove inactive**

Use this command to clean up unused installation files in case of insufficient space. Ensure that you have at least 1GB of space in flash to expand a new image.

```
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 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.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

a) **install add file activate commit**

Use this command to install the target image. You can point to the source image on your TFTP server or in flash if you have it copied to flash.

```
Switch# install add file flash:cat9k_iosxe.17.01.01.SPA.bin activate commit
_install_add_activate_commit: START Wed Nov 20 16:37:25 IST 2019

*Nov 20 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.17.01.01.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.17.01.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.01.01.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: 17.1.1
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 may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on Active/Standby

*Nov 20 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


*Nov 20 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  Wed Nov 20 16:46:18 IST 2019
```

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

b) **dir flash:**

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

```
Switch# dir flash:*.pkg
Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104    Jul 29 2019 09:52:41 -07:00 cat9k-cc_srdriver.16.12.01.SPA.pkg
475141 -rw- 70333380   Jul 29 2019 09:52:44 -07:00 cat9k-espbase.16.12.01.SPA.pkg
475142 -rw- 13256      Jul 29 2019 09:52:44 -07:00 cat9k-guestshell.16.12.01.SPA.pkg
475143 -rw- 349635524  Jul 29 2019 09:52:54 -07:00 cat9k-rpbase.16.12.01.SPA.pkg
475149 -rw- 24248187   Jul 29 2019 09:53:02 -07:00 cat9k-rpboot.16.12.01.SPA.pkg
475144 -rw- 25285572   Jul 29 2019 09:52:55 -07:00 cat9k-sipbase.16.12.01.SPA.pkg
475145 -rw- 20947908   Jul 29 2019 09:52:55 -07:00 cat9k-sipspa.16.12.01.SPA.pkg
475146 -rw- 2962372    Jul 29 2019 09:52:56 -07:00 cat9k-srdriver.16.12.01.SPA.pkg
475147 -rw- 13284288   Jul 29 2019 09:52:56 -07:00 cat9k-webui.16.12.01.SPA.pkg
475148 -rw- 13248      Jul 29 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 (8963174400 bytes free)
```

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.16.12.01.SPA.conf`— a backup copy of the newly installed packages.conf file

```
Switch# dir flash:*.conf

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

16631  -rw-             4882  Nov 20 2019 05:39:42 +00:00  packages.conf
16634  -rw-            4882  Nov 20 2019 05:34:06 +00:00  cat9k_iosxe.17.01.01.SPA.conf
```

Step 5 **upgrade rom-monitor capsule golden switch**

Use this command to upgrade the ROMMON version. After you enter the command, confirm upgrade at the system prompt.

For more information about this, see Upgrading the ROMMON, on page 11 in this document.

```
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 6 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 Amsterdam 17.1.1 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.
<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 via " 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 Amsterdam 17.1.1	Cisco IOS XE Gibraltar 16.12.1 or an earlier release.

The sample output in this section shows downgrade from Cisco IOS XE Amsterdam 17.1.1 to Cisco IOS XE Gibraltar 16.12.1, using **install** commands.

Important 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.

Procedure

Step 1 Clean Up

a) **install remove inactive**

Use this command to clean up unused installation files in case of insufficient space. Ensure that you have at least 1GB of space in flash to expand a new image.

```
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 Nov 20 2019 20:52:25 -07:00 cat9k_iosxe.16.12.01.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Downgrade software image

a) **install add file activate commit**

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. You can point to the source image on your tftp server or in flash if you have it copied to flash.

```
Switch# install add file flash:cat9k_iosxe.16.12.01.SPA.bin activate commit
_install_add_activate_commit: START Wed Nov 20 21:37:25 IST 2019

*Nov 20 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.16.12.01.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.16.12.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.16.12.01.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: 16.12.1
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 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  Wed Nov 20 21:46:18 IST 2019
```

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 does not automatically downgrade. It remains 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 (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Wed 20-Nov-19 22:38 by mcpre
<output truncated>
```

Licensing

This section provides information about the licensing packages for features available on Cisco Catalyst 9000 Series Switches.

License Levels

The software features available on Cisco Catalyst 9600 Series Switches fall under these base or add-on license levels.

Base Licenses

- Network Advantage

Add-On Licenses

Add-On Licenses require a Network Essentials or Network Advantage as a pre-requisite. The features available with add-on license levels provide Cisco innovations on the switch, as well as on the Cisco Digital Network Architecture Center (Cisco DNA Center).

- DNA Advantage

To find information about platform support and to know which license levels a feature is available with, use Cisco Feature Navigator. To access Cisco Feature Navigator, go to https://cfnng.cisco.com. An account on cisco.com is not required.

License Types

The following license types are available:

- Permanent—for a license level, and without an expiration date.
- Term—for a license level, and for a three, five, or seven year period.
- Evaluation—a license that is not registered.

License Levels - Usage Guidelines

- Base licenses (Network-Advantage) are ordered and fulfilled only with a permanent license type.

- Add-on licenses (DNA Advantage) are ordered and fulfilled only with a term license type.
- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- Evaluation licenses cannot be ordered. They are not tracked via Cisco Smart Software Manager and expire after a 90-day period. Evaluation licenses can be used only once on the switch and cannot be regenerated. Warning system messages about an evaluation license expiry are generated only 275 days after expiration and every week thereafter. An expired evaluation license cannot be reactivated after reload. This applies only to *Smart Licensing*. The notion of evaluation licenses does not apply to *Smart Licensing Using Policy*.

Cisco Smart Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- Unified Management: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (http://software.cisco.com).

Important Cisco Smart Licensing is the default and the only available method to manage licenses.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Deploying Smart Licensing

The following provides a process overview of a day 0 to day N deployment directly initiated from a device. Links to the configuration guide provide detailed information to help you complete each one of the smaller tasks.

Procedure

Step 1 Begin by establishing a connection from your network to Cisco Smart Software Manager on cisco.com.

In the software configuration guide of the required release, see *System Management* → *Configuring Smart Licensing* → *Connecting to CSSM*

Step 2 Create and activate your Smart Account, or login if you already have one.

To create and activate Smart Account, go to Cisco Software Central → Create Smart Accounts. Only authorized users can activate the Smart Account.

Step 3 Complete the Cisco Smart Software Manager set up.

a) Accept the Smart Software Licensing Agreement.

b) Set up the required number of Virtual Accounts, users and access rights for the virtual account users.

Virtual accounts help you organize licenses by business unit, product type, IT group, and so on.

c) Generate the registration token in the Cisco Smart Software Manager portal and register your device with the token.

In the software configuration guide of the required release, see *System Management → Configuring Smart Licensing → Registering the Device in CSSM*

With this,

- The device is now in an authorized state and ready to use.
- The licenses that you have purchased are displayed in your Smart Account.

Using Smart Licensing on an Out-of-the-Box Device

If an out-of-the-box device has the software version factory-provisioned, all licenses on such a device remain in evaluation mode until registered in Cisco Smart Software Manager.

In the software configuration guide of the required release, see *System Management → Configuring Smart Licensing → Registering the Device in CSSM*

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

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.
- Hardware Limitatons — Optics:

- Copper cables are not supported with 25GE, 40GE, and 100GE configurations
- Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapater —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 adapater — 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.

- Hardware Limitatons — 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)
  - 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.
- 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.

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	Description
CSCvq72472	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvr88090	Cat9300 crash on running show platform software fed switch 1 fss abstraction
CSCvr90477	9500 incorrectly set more-fragment flag for double fragmentation
CSCvr92287	EPC with packet-len opt breaks CPU in-band path for bigger frames
CSCvr92660	STP BPDUs not being sent from FED to IOSd
CSCvr98281	After valid ip conflict, SVI admin down responds to GARP
CSCvr99132	SPANed multicast packet reduced TTL
CSCvs08369	interface bringup delayed by a minute with large no. of SFPs installed

Identifier	Description
CSCvs14893	802.1x-MultiAuth/MultiDomain: C9K - Traffic drop in egress direction for Data-Vlan on a Auth port
CSCvs23505	9600 Auto upgrade on HA doesnt get triggered incase of version mismatch

Resolved Caveats in Cisco IOS XE Amsterdam 17.1.1

Identifier	Description
CSCvo66246	Enabling SPAN source of VLAN 1 affects LACP operations
CSCvp71508	Cat9500HP has same mac-address on mgmt port and first asic port after reload
CSCvp84502	ERSPAN destination does not work or forward traffic
CSCvq05337	Cat9500 || v169_3_hemit_es_throttle ES image || EGR_INVALID_REWRITE counter increasing in mVPN setup
CSCvq13053	NAT translation entry not cleared after fin-rst time-out
CSCvq22224	cat9k // evpn/vxlan // dhcp relay not working over l3vni
CSCvq43450	C9400 Sup uplinks with netflow configuration stopped forwarding traffic after switchover
CSCvq55973	C9600 - All Line cards shut down due to insufficient power and recover back in few mins
CSCvq58991	C9400/16.11.1 - Diagnostic test of TestPortTxMonitoring is failing for DAD links
CSCvq72181	16.12.1 - Seeing 100% CPU with FED on 9500 SVL setup
CSCvq72713	Cat3k/Cat9k can't forwarding traffic follow the rule of EIGRP unequal cost load-balancing
CSCvq93773	C9600/9400/9500H/9300 etc crashes due to CMCC heartbeat failures
CSCvr04551	Multicast stream flickers on igmp join/leave
CSCvr07162	system crash on execute "fed TCAM utilization"
CSCvr20139	Packet loss and FSC/RCV Error seen when pumping with mgig IXIA card (1518-9216bytes)
CSCvr55472	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 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: http://www.cisco.com/go/mibs

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact 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.