Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Bengaluru 17.6.x

First Published: 2021-08-02

Last Modified: 2024-04-06

Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Bengaluru 17.6.x

Introduction

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

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

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

Whats New In Cisco IOS XE Bengaluru 17.6.8

Hardware Features in Cisco IOS XE Bengaluru 17.6.8

There are no new hardware features in this release.

Software Features in Cisco IOS XE Bengaluru 17.6.8

There are no new software features in this release.

Whats New in Cisco IOS XE Bengaluru 17.6.7

Hardware Features in Cisco IOS XE Bengaluru 17.6.7

There are no new hardware features in this release.

Software Features in Cisco IOS XE Bengaluru 17.6.7

There are no new software features in this release.

Whats New in Cisco IOS XE Bengaluru 17.6.6a

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

Whats New in Cisco IOS XE Bengaluru 17.6.6

Hardware Features in Cisco IOS XE Bengaluru 17.6.6

There are no new hardware features in this release.

Software Features in Cisco IOS XE Bengaluru 17.6.6

There are no new software features in this release.

Whats New in Cisco IOS XE Bengaluru 17.6.5

Hardware Features in Cisco IOS XE Bengaluru 17.6.5

There are no new hardware features in this release.

Software Features in Cisco IOS XE Bengaluru 17.6.5

There are no new software features in this release.

Whats New in Cisco IOS XE Bengaluru 17.6.4

Hardware Features in Cisco IOS XE Bengaluru 17.6.4

There are no hardware features in this release.

Software Features in Cisco IOS XE Bengaluru 17.6.4

There are no new software features in this release.

Whats New in Cisco IOS XE Bengaluru 17.6.3

Hardware Features in Cisco IOS XE Bengaluru 17.6.3

There are no new hardware features in this release.

Software Features in Cisco IOS XE Bengaluru 17.6.3

There are no new software features in this release.

Whats New in Cisco IOS XE Bengaluru 17.6.2

Hardware Features in Cisco IOS XE Bengaluru 17.6.2

There are no new hardware features in this release.

Software Features in Cisco IOS XE Bengaluru 17.6.2

Feature Name	Description and License Level Information
Data MDT Support for L3 TRM	Introduces support for data multicast distribution tree (MDT) for Layer 3 Tenant Routed Multicast (TRM). Data MDTs are purpose built underlay MDTs to provide optimized forwarding in the MVPN and EVPN core. See BGP EVPN VXLAN → Configuring Tenant Routed Multicast. (Network Advantage)

Whats New in Cisco IOS XE Bengaluru 17.6.1

Hardware Features in Cisco IOS XE Bengaluru 17.6.1

Feature Name	Description and Documentation Link
10GBASE-CU SFP+ Cable	Supported cable product numbers: SFP-H10GB-CU4M 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 Bengaluru 17.6.1

Feature Name	Description and License Level Information
IPv6 Explicit Null Label	Allows you to use IPv6 Explicit Null Label as a VPN label to exchange IPv6 reachability information over the MPLS core. The label has a value of 2. (Network Advantage)
MLD Snooping over VPLS	Introduces support for Multicast Listener Discovery (MLD) Snooping over Virtual Private LAN Services (VPLS). This feature allows traffic to be forwarded over pseudowires that receive Internet Group Management Protocol (IGMP) or MLD reports from remote provider edge (PE) devices. (Network Advantage)
MPLS Traffic Engineering • IP Explicit Address Exclusion • LSP Attributes • Bundled Interface • Configurable Path Calculation Metric for Tunnels	Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) provides an integrated approach to traffic engineering by incorporating capabilities of Layer 2 into Layer 3. • IP Explicit Address Exclusion: Provides a means to exclude a link or node from the path for MPLS TE label switched path (LSP). • LSP Attributes: Provides an LSP Attribute List feature and a Path Option for Bandwidth Override feature. • Bundled Interface: Enables MPLS Traffic Engineering tunnels over the bundled interfaces, EtherChannel and Gigabit EtherChannel. • Configurable Path Calculation Metric for Tunnels: Enables the user to control the metric used in path calculation for traffic engineering tunnels on a per-tunnel basis. (Network Advantage)
Programmability • NETCONF Access from Guest Shell • YANG Data Models	The following programmability features are introduced in this release: • NETCONF Access from Guest Shell: Introduces support for accessing NETCONF from within the Guest Shell, to run Python scripts and invoke Cisco-custom package CLIs using the NETCONF protocol. (DNA Essentials and DNA Advantage) • 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/1761. 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.
RadSec CoA over same tunnel	Introduces support for RadSec Change of Authorization (CoA) request reception and CoA response transmission over the same authentication channel. (Network Essentials and Network Advantage)

Feature Name	Description and License Level Information
SCP improvement in large RTT scenario	Introduces support for secure copy (SCP) in large round trip time (RTT) settings by using the window-size variable option of the **ip ssh bulk-mode** command. (Network Essentials and Network Advantage)
Static NAT precedence over Dynamic NAT rule	Allows static NAT rule to precede over dynamic NAT rule when a given address is eligible for translation by both the rules. (Network Advantage)
WCCP - VRF support	Introduces support for virtual routing and forwarding (VRF) with Web Cache Communication Protocol (WCCP). (Network Advantage)
SSO Support for VRRPv3	Introduces support for Stateful Switchover (SSO) with Virtual Router Redundancy Protocol version 3 (VRRPv3). Use the **fhrp sso** command to enable this feature. (Network Essentials and Network Advantage)

New on the WebUI	
BFD Echo Mode for OSPFv3	Provides a mechanism to detect failures in the network between two adjacent switches, including the interfaces, data links, and forwarding planes. This feature can be configured globally, or per interface.
SDM Templates	Introduces device specific custom SDM templates that help to optimise the use of physical resources on the device.

Serviceability	
show consistency-checker	The command was modified. The following keywords were introduced: • **mcast**: Runs the consistency-checker on the multicast forwarding tables • **objects**: Runs the consistency-checker on objects • **run-id**: Runs the consistency-checker by run ID
show platform nat translations	The command was introduced. It records and displays all NAT sessions for monitoring and troubleshooting.
show platform nat translations statistics	The command was introduced. It displays current NAT statistics, including the NAT active sessions.
match device-type regex *regular-expression*	The command was modified. **regex** keyword was introduced. It allows you to define a regular expression for the device type.
protocol **tlv-type** *number* **value** {*string* | *integer* | {**regex** *regular-expression*}}	The command was modified. **regex** keyword was introduced. It allows you to define a regular expression for the Type-Length-Value (TLV).

Important Notes

- Unsupported Features, on page 6
- Complete List of Supported Features, on page 6
- Accessing Hidden Commands, on page 6
- Default Behaviour, on page 7

Unsupported Features

- 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://cfnng.cisco.com.

Accessing Hidden Commands

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

Hidden commands are available under:

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

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

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

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

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

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

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

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

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

Default Behaviour

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

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

Product ID (append with "=" for spares)	Description
C9K-F2-SSD-960GB	Cisco Catalyst 9600 Series 960GB SSD Storage
Line Cards	
C9600-LC-48YL	Cisco Catalyst 9600 Series 48-Port SFP56 line card. • C9600X-SUP-2 • 48 SFP56 ports of 50G/25G/10G • C9600X-SUP-1 • 48 SFP28 ports of 25G/10G/1G
C9600-LC-24C	Cisco Catalyst 9600 Series 24-Port 40G/12-Port 100G line card. • C9600X-SUP-2 • 24 QSFP28 ports of 100G/40G • C9600-SUP-1 • 12 ports of 100G or 24 ports of 40G
C9600-LC-48TX	Cisco Catalyst 9600 Series 48-Port MultiGigabit RJ45 line card. • C9600X-SUP-2 • 48 ports of 10G/5G/2.5G • C9600X-SUP-1 • 48 ports of 10G/5G/2.5G/1G and 100M/10M
C9600-LC-48S	Cisco Catalyst 9600 Series 48-Port SFP line card. • C9600X-SUP-2 • Not supported • C9600-SUP-1 • 48 SFP ports of 1G
AC Power Supply Modules	
C9600-PWR-2KWAC	Cisco Catalyst 9600 Series 2000W AC Power Supply Module[3]
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

To view the software compatibility information between Cisco Catalyst 9600 Series Switches, Cisco Identity Services Engine, and Cisco Prime Infrastructure, go to Cisco Catalyst 9000 Series Switches Software Version Compatibility Matrix.

Web UI System Requirements

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

Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[4]	512 MB[5]	256	1280 x 800 or higher	Small

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

Software Requirements

Operating Systems

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

Browsers

- Google Chrome—Version 59 or later (On Windows and Mac)
- Microsoft Edge
- Mozilla Firefox—Version 54 or later (On Windows and Mac)
- Safari—Version 10 or later (On Mac)

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)
Bengaluru 17.6.8	17.6.1r	-
Bengaluru 17.6.7	17.6.1r	-
Bengaluru 17.6.6a	17.6.1r	-
Bengaluru 17.6.6	17.6.1r	-
Bengaluru 17.6.5	17.6.1r	-
Bengaluru 17.6.4	17.6.1r	-
Bengaluru 17.6.3	17.6.1r	-
Bengaluru 17.6.2	17.6.1r	-
Bengaluru 17.6.1	17.6.1r	-
Bengaluru 17.5.1	17.3.1r[FC2]	-
Bengaluru 17.4.1	17.3.1r[FC2]	-
Amsterdam 17.3.8a	17.3.1r[FC2]	-
Amsterdam 17.3.8	17.3.1r[FC2]	-
Amsterdam 17.3.7	17.3.1r[FC2]	-
Amsterdam 17.3.6	17.3.1r[FC2]	-
Amsterdam 17.3.5	17.3.1r[FC2]	-
Amsterdam 17.3.4	17.3.1r[FC2]	-

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

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 Bengaluru 17.6.8	CAT9K_IOSXE	cat9k_lite_iosxe.17.06.08.S
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.06.08.
Cisco IOS XE Bengaluru 17.6.7	CAT9K_IOSXE	cat9k_iosxe.17.06.07.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.06.07.
Cisco IOS XE Bengaluru 17.6.6a	CAT9K_IOSXE	cat9k_iosxe.17.06.06a.SPA
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.06.06a

Release	Image Type	File Name
Cisco IOS XE Bengaluru 17.6.6	CAT9K_IOSXE	cat9k_iosxe.17.06.06.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.06.06.SPA
Cisco IOS XE Bengaluru 17.6.5	CAT9K_IOSXE	cat9k_iosxe.17.06.05.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.06.05.SPA
Cisco IOS XE Bengaluru 17.6.4	CAT9K_IOSXE	cat9k_iosxe.17.06.04.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.06.04.SPA
Cisco IOS XE Bengaluru 17.6.3	CAT9K_IOSXE	cat9k_iosxe.17.06.03.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.06.03.SPA
Cisco IOS XE Bengaluru 17.6.2	CAT9K_IOSXE	cat9k_iosxe.17.06.02.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.06.02.SPA
Cisco IOS XE Bengaluru 17.6.1	CAT9K_IOSXE	cat9k_iosxe.17.06.01.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.06.01.SPA

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.

- Upgrading the ROMMON in the golden SPI flash device

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

Note

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

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

Software Installation Commands

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

Upgrading in Install Mode

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

Before you begin

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

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

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

When upgrading from ...	To...
Cisco IOS XE Bengaluru 17.5.x or earlier releases	Cisco IOS XE Bengaluru 17.6.x

The sample output in this section displays upgrade from Cisco IOS XE Bengaluru 17.5.1 to Cisco IOS XE Bengaluru 17.6.1 using **install** commands.

Procedure

Step 1 Clean-up

install remove inactive

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

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

```
Switch# install remove inactive
install_remove: START Fri Jul 23 19:51:48 UTC 2021
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
    cat9k-cc_srdriver.17.05.01.SPA.pkg
      File is in use, will not delete.
    cat9k-espbase.17.05.01.SPA.pkg
      File is in use, will not delete.
    cat9k-guestshell.17.05.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpbase.17.05.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpboot.17.05.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipbase.17.05.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipspa.17.05.01.SPA.pkg
      File is in use, will not delete.
    cat9k-srdriver.17.05.01.SPA.pkg
      File is in use, will not delete.
    cat9k-webui.17.05.01.SPA.pkg
      File is in use, will not delete.
    cat9k-wlc.17.05.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.17.05.01.SPA.pkg
/flash/cat9k-espbase.17.05.01.SPA.pkg
/flash/cat9k-guestshell.17.05.01.SPA.pkg
/flash/cat9k-rpbase.17.05.01.SPA.pkg
/flash/cat9k-rpboot.17.05.01.SPA.pkg
/flash/cat9k-sipbase.17.05.01.SPA.pkg
/flash/cat9k-sipspa.17.05.01.SPA.pkg
/flash/cat9k-srdriver.17.05.01.SPA.pkg
/flash/cat9k-webui.17.05.01.SPA.pkg
/flash/cat9k-wlc.17.05.01.SPA.pkg
/flash/packages.conf

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

[switch 1]:
```

```
Deleting file flash:cat9k-cc_srdriver.17.05.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.17.05.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.17.05.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.17.05.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.05.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.17.05.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.17.05.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.17.05.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.17.05.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.17.05.01.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 Fri Jul 23 19:52:25 UTC 2021
Switch#
```

Step 2 Copy new image to flash

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

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

```
Switch# copy tftp://10.8.0.6/image/cat9k_iosxe.17.06.01.SPA.bin flash:
destination filename [cat9k_iosxe.17.06.01.SPA.bin]?
Accessing tftp://10.8.0.6/image/cat9k_iosxe.17.06.01.SPA.bin...
Loading /cat9k_iosxe.17.06.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]

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

b) **dir flash:*.bin**

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

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

Directory of flash:/

434184 -rw- 601216545    Jul 23 2021 10:18:11 -07:00 cat9k_iosxe.17.06.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

Step 3 Set boot variable

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

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

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

b) **no boot manual**

Use this command to configure the switch to auto-boot. Settings are synchronized with the standby switch, if applicable.

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

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show bootvar**

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

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

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

Step 4 Install image to flash

install add file activate commit

Use this command to install the image.

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

The following sample output displays installation of the Cisco IOS XE Bengaluru 17.6.1 software image to flash:

```
Switch# install add file flash:cat9k_iosxe.17.06.01.SPA.bin activate commit
_install_add_activate_commit: START Fri Jul 23 16:37:25 IST 2021

*Jul 23 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.17.06.01.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.17.06.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.06.01.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: 17.6.01

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.06.01.SPA.pkg
/flash/cat9k-webui.17.06.01.SPA.pkg
/flash/cat9k-srdriver.17.06.01.SPA.pkg
/flash/cat9k-sipspa.17.06.01.SPA.pkg
/flash/cat9k-sipbase.17.06.01.SPA.pkg
/flash/cat9k-rpboot.17.06.01.SPA.pkg
/flash/cat9k-rpbase.17.06.01.SPA.pkg
/flash/cat9k-guestshell.17.06.01.SPA.pkg
/flash/cat9k-espbase.17.06.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.06.01.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
*Jul 23 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

*Jul 23 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  Fri Jul 23 16:46:18 IST 2021
```

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

Step 5 Verify installation

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

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

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

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

```
475140 -rw- 2012104    Mar 19 2021 09:52:41 -07:00 cat9k-cc_srdriver.17.05.01.SPA.pkg
475141 -rw- 70333380   Mar 19 2021 09:52:44 -07:00 cat9k-espbase.17.05.01.SPA.pkg
475142 -rw- 13256      Mar 19 2021 09:52:44 -07:00 cat9k-guestshell.17.05.01.SPA.pkg
475143 -rw- 349635524  Mar 19 2021 09:52:54 -07:00 cat9k-rpbase.17.05.01.SPA.pkg
475149 -rw- 24248187   Mar 19 2021 09:53:02 -07:00 cat9k-rpboot.17.05.01.SPA.pkg
475144 -rw- 25285572   Mar 19 2021 09:52:55 -07:00 cat9k-sipbase.17.05.01.SPA.pkg
475145 -rw- 20947908   Mar 19 2021 09:52:55 -07:00 cat9k-sipspa.17.05.01.SPA.pkg
475146 -rw- 2962372    Mar 19 2021 09:52:56 -07:00 cat9k-srdriver.17.05.01.SPA.pkg
475147 -rw- 13284288   Mar 19 2021 09:52:56 -07:00 cat9k-webui.17.05.01.SPA.pkg
475148 -rw- 13248      Mar 19 2021 09:52:56 -07:00 cat9k-wlc.17.05.01.SPA.pkg

491524 -rw- 25711568   Jul 23 2021 11:49:33 -07:00  cat9k-cc_srdriver.17.06.01.SPA.pkg
491525 -rw- 78484428   Jul 23 2021 11:49:35 -07:00  cat9k-espbase.17.06.01.SPA.pkg
491526 -rw- 1598412    Jul 23 2021 11:49:35 -07:00  cat9k-guestshell.17.06.01.SPA.pkg
491527 -rw- 404153288  Jul 23 2021 11:49:47 -07:00  cat9k-rpbase.17.06.01.SPA.pkg
491533 -rw- 31657374   Jul 23 2021 11:50:09 -07:00  cat9k-rpboot.17.06.01.SPA.pkg
491528 -rw- 27681740   Jul 23 2021 11:49:48 -07:00  cat9k-sipbase.17.06.01.SPA.pkg
491529 -rw- 52224968   Jul 23 2021 11:49:49 -07:00  cat9k-sipspa.17.06.01.SPA.pkg
491530 -rw- 31130572   Jul 23 2021 11:49:50 -07:00  cat9k-srdriver.17.06.01.SPA.pkg
491531 -rw- 14783432   Jul 23 2021 11:49:51 -07:00  cat9k-webui.17.06.01.SPA.pkg
491532 -rw- 9160       Jul 23 2021 11:49:51 -07:00  cat9k-wlc.17.06.01.SPA.pkg

11353194496 bytes total (8963174400 bytes free)
```

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

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

- `packages.conf`—the file that has been re-written with the newly installed .pkg files.
- `cat9k_iosxe.17.06.01.SPA.conf`— a backup copy of the newly installed packages.conf file.

```
Switch# dir flash:*.conf

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

16631  -rw- 4882 Jul 23 2021 05:39:42 +00:00  packages.conf
16634  -rw- 4882 Jul 23 2021 05:34:06 +00:00  cat9k_iosxe.17.06.01.SPA.conf
```

Step 6 Verify version

show version

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

The following sample output of the **show version** command displays the Cisco IOS XE Bengaluru 17.6.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.06.01
Cisco IOS Software [Bengaluru], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.6.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc..
<output truncated>
```

Downgrading in Install Mode

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

Before you begin

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

When downgrading from ...	To ...
Cisco IOS XE Bengaluru 17.6.x	Cisco IOS XE Bengaluru 17.5.x or earlier releases.

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

The sample output in this section shows downgrade from Cisco IOS XE Bengaluru 17.6.1 to Cisco IOS XE Bengaluru 17.5.1, using **install** commands.

Procedure

Step 1 Clean-up

install remove inactive

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

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

```
Switch# install remove inactive
 install_remove: START Fri Jul 23 11:42:27 IST 2021

Cleaning up unnecessary package files

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

Cleaning bootflash:
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat9k-cc_srdriver.17.06.01.SSA.pkg
      File is in use, will not delete.
    cat9k-espbase.17.06.01.SSA.pkg
      File is in use, will not delete.
    cat9k-guestshell.17.06.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpbase.17.06.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpboot.17.06.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipbase.17.06.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipspa.17.06.01.SSA.pkg
```

```
      File is in use, will not delete.
    cat9k-srdriver.17.06.01.SSA.pkg
      File is in use, will not delete.
    cat9k-webui.17.06.01.SSA.pkg
      File is in use, will not delete.
    cat9k-wlc.17.06.01.SSA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.
SUCCESS: No extra package or provisioning files found on media. Nothing to clean.

SUCCESS: install_remove  Fri Jul 23 11:42:39 IST 2021

--- 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 Fri Jul 23 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

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

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

```
Switch# copy tftp://10.8.0.6/image/cat9k_iosxe.17.05.01.SPA.bin flash:
Destination filename [cat9k_iosxe.17.05.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.17.05.01.SPA.bin...
Loading /cat9k_iosxe.17.05.01.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 23 2021 13:35:16 -07:00 cat9k_iosxe.17.05.01.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Set boot variable

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

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

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

b) **no boot manual**

Use this command to configure the switch to auto-boot. Settings are synchronized with the standby switch, if applicable.

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

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show bootvar**

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

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

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

Step 4 Downgrade software image

install add file activate commit

Use this command to install the image.

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

The following example displays the installation of the Cisco IOS XE Bengaluru 17.5.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.17.05.01.SPA.bin activate commit
_install_add_activate_commit: START Fri Jul 23 21:37:25 IST 2021

*Jul 23 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.17.05.01.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.17.05.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.05.01.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: 17.05.1
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.05.01.SPA.pkg
/flash/cat9k-webui.17.05.01.SPA.pkg
/flash/cat9k-srdriver.17.05.01.SPA.pkg
/flash/cat9k-sipspa.17.05.01.SPA.pkg
/flash/cat9k-sipbase.17.05.01.SPA.pkg
/flash/cat9k-rpboot.17.05.01.SPA.pkg
/flash/cat9k-rpbase.17.05.01.SPA.pkg
/flash/cat9k-guestshell.17.05.01.SPA.pkg
/flash/cat9k-espbase.17.05.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.05.01.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

*Jul 23 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


*Jul 23 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  Fri Jul 23 21:46:18 IST 2021
```

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

Step 5 Verify version

show version

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

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

The following sample output of the **show version** command displays the Cisco IOS XE Bengaluru 17.5.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.05.01
Cisco IOS Software [Bengaluru], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.5.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
<output truncated>
```

In Service Software Upgrade (ISSU) with Cisco StackWise Virtual and Dual Supervisor Module Configuration

Follow the instructions described here to perform an In Service Software Upgrade (ISSU) upgrade. Use the procedure described here, only for the releases indicated in the table below. For more general information about ISSU release support and recommended releases, see this technical reference document: In-Service Software Upgrade (ISSU).

Before you begin

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

When upgrading from...	Use these commands...	To...
Cisco IOS XE Amsterdam 17.3.x	**install add file activate issu commit**	Cisco IOS XE Bengaluru 17.6.x
Not applicable	ISSU does not support downgrade. To downgrade, see Downgrading in Install Mode, on page 19.	Not applicable

Procedure

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Switch# enable
```

Step 2 **install add file activate issu commit**

Use this command to automate the sequence of all the upgrade procedures, including downloading the images to both the switches, expanding the images into packages, and upgrading each switch as per the procedures.

```
Switch# install add file tftp:cat9k_iosxe.17.06.01.SPA.bin activate issu commit
```

The following sample output displays installation of Cisco IOS XE Amsterdam 17.3.2a software image with ISSU procedure.

```
Switch# install add file tftp:cat9k_iosxe.17.06.01.SPA.bin activate issu commit
install_add_activate_commit: START Thu Jul 19 06:16:32 UTC 2021
Downloading file tftp://172.27.18.5//cat9k_iosxe.17.06.01.SPA.bin

*Jul 19 06:16:34.064: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine: Started
 install one-shot ISSU tftp://172.27.18.5//cat9k_iosxe.17.06.01.SPA.bin
Finished downloading file tftp://172.27.18.5//cat9k_iosxe.17.06.01.SPA.bin to
```

```
flash:cat9k_iosxe.17.06.01.SPA.bin
install_add_activate_commit: Adding ISSU

--- Starting initial file syncing ---
[1]: Copying flash:cat9k_iosxe.17.06.01.SPA.bin from switch 1 to switch 2
[2]: Finished copying to switch 2
Info: Finished copying flash:cat9k_iosxe.17.06.01.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
  [2] Add package(s) on switch 2
  [2] Finished Add on switch 2
Checking status of Add on [1 2]
Add: Passed on [1 2]
Finished Add

install_add_activate_commit: Activating ISSU

NOTE: Going to start Oneshot ISSU install process

STAGE 0: Initial System Level Sanity Check before starting ISSU
================================================
--- Verifying install_issu supported ---
--- Verifying standby is in Standby Hot state ---
--- Verifying booted from the valid media ---
--- Verifying AutoBoot mode is enabled ---
Finished Initial System Level Sanity Check


STAGE 1: Installing software on Standby
================================================
--- Starting install_remote ---
Performing install_remote on Chassis remote
[2] install_remote package(s) on switch 2
[2] Finished install_remote on switch 2
install_remote: Passed on [2]
Finished install_remote


STAGE 2: Restarting Standby
================================================
--- Starting standby reload ---
Finished standby reload

--- Starting wait for Standby to reach terminal redundancy state ---

*Jul 19 06:24:16.426: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Jul 19 06:24:16.426: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Jul 19 06:24:16.466: %HMANRP-5-CHASSIS_DOWN_EVENT: Chassis 2 gone DOWN!
*Jul 19 06:24:16.497: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_NOT_PRESENT)
*Jul 19 06:24:16.498: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN)
*Jul 19 06:24:16.498: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
*Jul 19 06:24:16.674: %RF-5-RF_RELOAD: Peer reload. Reason: EHSA standby down
*Jul 19 06:24:16.679: %IOSXE_REDUNDANCY-6-PEER_LOST: Active detected switch 2 is no longer
 standby
*Jul 19 06:24:16.416: %NIF_MGR-6-PORT_LINK_DOWN: Switch 1 R0/0: nif_mgr: Port 1 on front
side stack link 0 is DOWN.
*Jul 19 06:24:16.416: %NIF_MGR-6-PORT_CONN_DISCONNECTED: Switch 1 R0/0: nif_mgr: Port 1 on
 front side stack link 0 connection has DISCONNECTED: CONN_ERR_PORT_LINK_DOWN_EVENT
*Jul 19 06:24:16.416: %NIF_MGR-6-STACK_LINK_DOWN: Switch 1 R0/0: nif_mgr: Front side stack
```

```
 link 0 is DOWN.
*Jul 19 06:24:16.416: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack port
1 on Switch 1 is down

<output truncated>

*Jul 19 06:29:36.393: %IOSXE_REDUNDANCY-6-PEER: Active detected switch 2 as standby.
*Jul 19 06:29:36.392: %STACKMGR-6-STANDBY_ELECTED: Switch 1 R0/0: stack_mgr: Switch 2 has
been elected STANDBY.
*Jul 19 06:29:41.397: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_FOUND(4))
*Jul 19 06:29:41.397: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
*Jul 19 06:29:42.257: %REDUNDANCY-3-IPC: IOS versions do not match.
*Jul 19 06:30:24.323: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeededFinished
wait for Standby to reach terminal redundancy state


*Jul 19 06:30:25.325: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
STAGE 3: Installing software on Active
==================================================
--- Starting install_active ---
Performing install_active on Chassis 1

<output truncated>

[1] install_active package(s) on switch 1
[1] Finished install_active on switch 1
install_active: Passed on [1]
Finished install_active


STAGE 4: Restarting Active (switchover to standby)
==================================================
--- Starting active reload ---
New software will load after reboot process is completed
SUCCESS: install_add_activate_commit  Thu Jul 19 23:06:45 UTC 2021
Jul 19 23:06:45.731: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot ISSU flash:cat9k_iosxe.17.06.01.SPA.bin
Jul 19 23:06:47.509: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
Jul 19 23:06:48.776: %PM

Initializing Hardware...

System Bootstrap, Version 17.3.1r[FC2], RELEASE SOFTWARE (P)
Compiled Fri 08/17/2018 10:48:42.68 by rel

Current ROMMON image : Primary
Last reset cause     : PowerOn
C9500-40X platform with 16777216 Kbytes of main memory

boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf
#
################################################################################################################################



Jul 19 23:08:30.238: %PMAN-5-EXITACTION: C0/0: pvp: Process manager is exiting:

Waiting for 120 seconds for other switches to boot
######################
Switch number is 1
```

```
All switches in the stack have been discovered. Accelerating discovery


Switch console is now available

Press RETURN to get started.




Jul 19 23:14:17.080: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
commit
Jul 19 23:15:48.445: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install commit ISSU
```

Step 3 **show version**

Use this command to verify the version of the new image.

The following sample output of the **show version** command displays the Cisco IOS XE Amsterdam 17.3.2a image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.06.01
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.6.1,
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
<output truncated>
```

Step 4 **show issu state** [*detail*]

Use this command to verify that no ISSU process is in pending state.

```
Switch# show issu state detail
--- Starting local lock acquisition on chassis 2 ---
Finished local lock acquisition on chassis 2

No ISSU operation is in progress

Switch#
```

Step 5 **exit**

Exits privileged EXEC mode and returns to user EXEC mode.

Field-Programmable Gate Array Version Upgrade

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

To check the current FPGA version, enter the **show firmware version all** command in 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.
- FPGA on Line Cards - 0x19070619

  FPGA version is upgraded only if the setup is reloaded. In case of upgrade with ISSU, the line card should be power-cycled for their FPGA to upgrade.

Licensing

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

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

Available Licensing Models and Configuration Information

- Cisco IOS XE Gibraltar 16.11.1 to Cisco IOS XE Amsterdam 17.3.1: Smart Licensing is the default and the only supported method to manage licenses.
- Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy, which is an enhanced version of Smart Licensing, is the default and the only supported method to manage licenses.

Scaling Guidelines

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

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

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

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

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 Limitations — Optics:

- Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapter —This adapter must not be installed on an even numbered port where the corresponding odd numbered port is configured as 40GE port. For example, if port 1 is configured as 40GE, CVR-QSFP-SFP10G must not be installed in port 2.

  Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapter — If you insert a 40-Gigabit Ethernet Transceiver Module to odd numbered port, the corresponding even numbered port does not work with CVR-QSFP-SFP10G adapter.

- GLC-T and GLC-TE operating at 10/100Mbps speed are not supported with Cisco QSA Module (CVR-QSFP-SFP10G).

- SFP-10G-T-X supports 100Mbps/1G/10G speeds based on auto negotiation with the peer device. You cannot force speed settings from the transceiver.

- Hardware Limitations — Power Supply Modules:
  - Input voltage for AC power supply modules—All AC-input power supply modules in the chassis must have the same AC-input voltage level.
  - Using power supply modules of different types—When mixing AC-input and DC-input power supplies, the AC-input voltage level must be 220 VAC.

- In-Service Software Upgrade (ISSU)
  - 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.

- Smart Licensing Using Policy: Starting with Cisco IOS XE Amsterdam 17.3.2a, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only

the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

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

- TACACS legacy command: Do not configure the legacy **tacacs-server host** command; this command is deprecated. If the software version running on your device is Cisco IOS XE Gibraltar 16.12.2 or a later release, using the legacy command can cause authentication failures. Use the **tacacs server** command in global configuration mode.
- USB Authentication—When you connect a Cisco USB drive to the switch, the switch tries to authenticate the drive against an existing encrypted preshared key. Since the USB drive does not send a key for authentication, the following message is displayed on the console when you enter **password encryption aes** command:

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

- MACsec is not supported on Software-Defined Access deployments.
- VLAN Restriction—It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.
- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.
- Embedded Event Manager—Identity event detector is not supported on Embedded Event Manager.
- 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 Bengaluru 17.6.x

Identifier	Headline
CSCwq83338	On the C9600 Dual-Sup, performing a redundancy force-switchover immediately after reaching STANDBY HOT causes the process to halt at "in progress to standby cold-config"

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.8

Identifier	Description
CSCwc67790	"verify bootflash:" command not able to process embedded hash in .bin file
CSCwi79020	Unexpected reload on C9K switch while running dot1X and device tracking

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.7

Identifier	Description
CSCwi37669	macro is getting pushed on closed and open auth ports when macro is global enabled
CSCwf10970	fed process crashing after AVB policy-map manipulation

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.6a

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

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.6

Identifier	Description
CSCwb76541	IOSd Crashes in "Call Home cert update" Process During Trustpool Download
CSCwd28734	Cat9k memory leak in pubd causes switch reload
CSCwe09745	Memory leak in Pubd when continuously trying to connect to remote peer
CSCwe95691	PnP | Cat9k sends DHCP Discover with IP Source address 192.168.1.1 instead of 0.0.0.0
CSCwe36743	Segmentation Fault - Crash - SSH - When Changing AAA Group Configs

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.5

There are no resolved caveats in this release.

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.4

Identifier	Description
CSCwa85199	High CPU Utilization and memory utilization by Smart Licensing Agent
CSCwb31319	C9600-LC-48TX High-Ipg Configuration May Cause Ports to Go Err-Disabled or Experience Packet Loss

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.3

Identifier	Description
CSCvv91195	1 Gigabit Fiber SFPs may not link up in C9600-LC-48YL module
CSCvy74900	Unexpected reload in HTTP CORE process
CSCvz51752	Randomly CTS enforcement not happening if multiple Tabs are used from the ISE to push COA
CSCvz60442	Unable to delete ip helper-address from the VLAN interface
CSCwa17969	Cat9k | standby unexpected reload when no ip helper-address global is executed
CSCwa49907	SG Brenton: 1G optics auto-negotiation failed when connected to peer SFF/SG LC ports from Brenton LC
CSCwa67012	Error seen when deleting ip igmp snooping querier
CSCwa67621	Cat9k with no SDG configuration routing mDNS traffic
CSCwa83315	IOS-FMAN-PTP ERROR: seen on console during issu

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.2

Identifier	Description
CSCvy64514	One of the SVL links using QSFP-40/100-SRBD 100G stuck on Suspended/Timout status after reload

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.1

There are no resolved caveats in this release.

Troubleshooting

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

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

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

Related Documentation

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

All support documentation for Cisco Catalyst 9600 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9600-series-switches/tsd-products-support-series-home.html

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

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

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

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

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

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

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.