Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS XE Bengaluru 17.6.x

First Published: 2021-08-02

Last Modified: 2024-04-06

Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS XE Bengaluru 17.6.x

Introduction

Cisco Catalyst 9200 Series Switches are entry level enterprise-class access switches that extend the power of intent-based networking and Cisco Catalyst 9000 Series Switches hardware and software innovation to a broader scale of deployments. These switches focus on offering features for the mid-market and simple branchdeployments. With its family pedigree, Cisco Catalyst 9200 Series Switches offer simplicity without compromise - it is secure, always on and provides IT simplicity.

As a foundational building block for Cisco Digital Network Architecture, this platform is built with security, mobility, cloud and IoT at its core. This gives you out of the box upgrades in security, resiliency and programmability regardless of where you are in the intent-based networking journey.

With access to Cisco's best in class security portfolio anchored trustworthy solutions, MACsec encryption and segmentation, the platform provides advanced security features that protect the integrity of the hardware as well as the software and all data that flows through the switch and the network. These switches provide enterprise-level resiliency and keep your business up and running seamlessly with field-replaceable power supplies and fans, modular uplinks, cold patching, perpetual PoE, and the industry's highest mean time between failures (MTBF). Combine the application visibility of full flexible NetFlow with telemetry and the open APIs of Cisco IOS XE and programmability of the UADP ASIC technology and these switches give you the best simple experience provisioning and managing your network now with investment protection on future innovations.

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

There are no new software features in this release.

Whats New in Cisco IOS XE Bengaluru 17.6.1

Hardware Features in Cisco IOS XE Bengaluru 17.6.1

There are no new hardware features in this release.

Software Features in Cisco IOS XE Bengaluru 17.6.1

Feature Name	Description and License Level Information
Programmability • FQDN Support for gRPC Subscriptions • NETCONF Access from Guest Shell • YANG Data Models	The following programmability features are introduced in this release: • FQDN Support for gRPC Subscriptions: Introduces support for FQDN for gRPC subscriptions feature, along with IP addresses. (Network Essentials and Network Advantage) • 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)

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 software fed switch punt packet-capture cpu-top-talker	The command was modified. **cpu-top-talker** keyword was introduced. It displays the occurrences of an attribute of a packet capture.
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

- Audio Video Bridging (including IEEE802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav)

- Border Gateway Protocol (BGP) including BGP EVPN VXLAN.
- Cisco StackWise Virtual
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Converged Access for Branch Deployments
- Fabric Enabled Wireless on C9200L SKUs
- Gateway Load Balancing Protocol (GLBP)
- Hot patching (for SMUs)
- IPsec VPN
- MACSec Encryption
  - MACsec configuration on EtherChannel
  - 256-bit AES MACsec (IEEE 802.1AE) host link encryption with MACsec Key Agreement (MKA)
- Multiprotocol Label Switching (MPLS)
- Non Stop Forwarding (NSF)
- Performance Monitoring (PerfMon)
- Private VLAN (PVLAN) on Trunks and Portchannels
- Programmability (Cisco Plug-in for OpenFlow 1.3, Third-Party Application Hosting)
- Virtual Routing and Forwarding (VRF)-Aware web authentication
- Web Cache Communication Protocol (WCCP)

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 9200 Series Switches—Model Numbers

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

[1] See Table: Table 1: Permitted Combinations, on page 24, for information about the add-on licenses that you can order.

Network Modules

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

Network Module	Description
C9200-NM-4G [1]	Four 1-GigabitEthernet SFP module slots
C9200-NM-4X [1]	Four 10-GigabitEthernet SFP+ module slots
C9200-NM-2Y[2]	Two 25-GigabitEthernet SFP28 module slots
C9200-NM-2Q[2]	Two 40-GigabitEthernet slots with a QSFP+ connector in each slot

Note These network modules are supported only on the C9200 SKUs of the Cisco Catalyst 9200 Series Switches.

Optics Modules

Cisco Catalyst Series Switches support a wide range of optics and the list of supported optics is updated on a regular basis. Use the Transceiver Module Group (TMG) Compatibility Matrix tool, or consult the tables at this URL for the latest transceiver module compatibility information: https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Compatibility Matrix

The following table provides software compatibility information between Cisco Catalyst 9200 Series Switches, Cisco Identity Services Engine, and Cisco Prime Infrastructure.

Catalyst 9200	Cisco Identity Services Engine	Cisco Prime Infrastructure
Bengaluru 17.6.7	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	C9200 and C9200L: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.6a	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	C9200 and C9200L: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.6	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	C9200 and C9200L: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.5	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	C9200 and C9200L: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.

Catalyst 9200	Cisco Identity Services Engine	Cisco Prime Infrastructure
Bengaluru 17.6.4	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	C9200 and C9200L: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.3	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	C9200 and C9200L: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.2	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	C9200 and C9200L: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.1	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Bengaluru 17.5.1	3.0 Patch 1 2.7 Patch 2 2.6 Patch 7 2.4 Patch 13	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Bengaluru 17.4.1	3.0 2.7 Patch 2	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Amsterdam 17.3.8a	2.7	C9200 and C9200L: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.

Catalyst 9200	Cisco Identity Services Engine	Cisco Prime Infrastructure
Amsterdam 17.3.8	2.7	C9200 and C9200L: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Amsterdam 17.3.7	2.7	C9200 and C9200L: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Amsterdam 17.3.6	2.7	C9200 and C9200L: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Amsterdam 17.3.5	2.7	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Amsterdam 17.3.4b	2.7	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Amsterdam 17.3.4	2.7	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Amsterdam 17.3.3	2.7	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Amsterdam 17.3.2a	2.7	C9200 and C9200L: PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See Cisco Prime Infrastructure 3.8 → **Downloads**.
Amsterdam 17.3.1	2.7	C9200 and C9200L: PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See Cisco Prime Infrastructure 3.8 → **Downloads**.
Amsterdam 17.2.1	2.7	C9200 and C9200L: PI 3.7 + PI 3.7 latest maintenance release + PI 3.7 latest device pack See Cisco Prime Infrastructure 3.7 → **Downloads**.
Amsterdam 17.1.1	2.7	C9200 and C9200L: PI 3.6 + PI 3.6 latest maintenance release + PI 3.6 latest device pack See Cisco Prime Infrastructure 3.6 → **Downloads**.

Catalyst 9200	Cisco Identity Services Engine	Cisco Prime Infrastructure
Gibraltar 16.12.8	2.6	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.7	2.6	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.6	2.6	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.5b	2.6	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.5	2.6	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.4	2.6	C9200 and C9200L: PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See Cisco Prime Infrastructure 3.8 → Downloads.
Gibraltar 16.12.3a	2.6	C9200 and C9200L: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.3	2.6	C9200 and C9200L: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.2	2.6	C9200 and C9200L: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.1	2.6	C9200 and C9200L: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.11.1	2.6 2.4 Patch 5	C9200 and C9200L: PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4 → **Downloads**.

Catalyst 9200	Cisco Identity Services Engine	Cisco Prime Infrastructure
Gibraltar 16.10.1	2.4	C9200: PI 3.4 + Device Pack 9 C9200L: PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.8	2.5 2.1	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.7	2.5 2.1	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.6	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.5	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.4	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.3	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.2[2]	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.

[2] The compatibility information for Fuji 16.9.2 applies only to the C9200L SKUs.

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[3]	512 MB[4]	256	1280 x 800 or higher	Small

[3] We recommend 1 GHz
[4] 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)

Boot Loader Versions

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

Release	ROMMON Version
Dublin 17.12.3	17.12.1r [FC3]
Bengaluru 17.6.7	17.9.1r [FC8]
Bengaluru 17.6.6a	17.9.1r [FC8]
Bengaluru 17.6.6	17.9.1r [FC8]
Bengaluru 17.6.5	17.9.1r [FC8]
Bengaluru 17.6.4	17.9.1r [FC8]
Bengaluru 17.6.3	17.8.1r [FC5]
Bengaluru 17.6.2	17.6.1r [FC1]
Bengaluru 17.6.1	17.6.1r [FC1]
Bengaluru 17.5.1	17.5.1r [FC4]
Bengaluru 17.4.1	17.4.1r [FC3]
Amsterdam 17.3.8a	17.9.1r [FC8]
Amsterdam 17.3.8	17.9.1r [FC8]
Amsterdam 17.3.7	17.9.1r [FC8]
Amsterdam 17.3.6	17.9.1r [FC8]
Amsterdam 17.3.5	17.5.1r [FC4]

Release	ROMMON Version
Amsterdam 17.3.4	17.5.1r [FC4]
Amsterdam 17.3.3	17.5.1r [FC4]
Amsterdam 17.3.2a	17.3.1r [FC4]
Amsterdam 17.3.1	17.3.1r [FC3]
Amsterdam 17.2.1	17.2.1r [FC2]
Amsterdam 17.1.1	17.1.1 [FC3]

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 17.6.7	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.06.07.S
Cisco IOS XE Bengaluru 17.6.6	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.06.06.S
Cisco IOS XE Bengaluru 17.6.5	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.06.05.S
Cisco IOS XE Bengaluru 17.6.4	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.06.04.S
Cisco IOS XE Bengaluru 17.6.3	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.06.03.S

Release	Image Type	File Name
Cisco IOS XE Bengaluru 17.6.2	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.06.02.SPA
Cisco IOS XE Bengaluru 17.6.1	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.06.01.SPA

Automatic Boot Loader Upgrade

When you upgrade from the existing release on your switch to a later or newer release for the first time, the boot loader may be automatically upgraded, based on the hardware version of the switch. If the boot loader is automatically upgraded, it will take effect on the next reload. If you go back to the older release after this, the boot loader is not downgraded. The updated boot loader supports all previous releases.

Caution Do not power cycle your switch during the upgrade.

Software Installation Commands

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

Upgrading in Install Mode

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

Before you begin

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

When upgrading from ...	To...
Cisco IOS XE 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 only.

Procedure

Step 1 Clean-up

install remove inactive

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

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

```
Switch# install remove inactive
install_remove: START Mon Jul 19 17:46:18 IST 2021
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat9k_lite-rpbase.17.05.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.17.05.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.17.05.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.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_lite_iosxe.17.05.01.SPA.bin

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

[switch 1]:
Deleting file flash:cat9k_lite_iosxe.17.05.01.SPA.bin ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
  [1] Post_Remove_Cleanup package(s) on switch 1
  [1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup
SUCCESS: install_remove  Mon Jul 19 17:47:20 IST 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_lite_iosxe.17.06.01.SPA.bin flash:

Destination filename [cat9k_lite_iosxe.17.06.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_lite_iosxe.17.06.01.SPA.bin...
Loading /cat9k_lite_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:**

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 19 2021 10:18:11 -07:00 cat9k_lite_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.

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

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show boot**

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

```
Switch# show boot
---------------------------
Switch 3
---------------------------
Current Boot Variables:
BOOT variable = flash:packages.conf;

Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = no
Enable Break = yes
Boot Mode = DEVICE
iPXE Timeout = 0
```

Step 4 Install image to flash

install add file activate commit

Use this command to install the image.

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

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

```
Switch# install add file flash:cat9k_lite_iosxe.17.06.01.SPA.bin activate commit
install_add_activate_commit: START Mon Jul 19 12:51:55 IST 2021
Jul 19 12:51:57.795: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
one-shot flash:cat9k_lite_iosxe.17.06.01.SPA.bininstall_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_lite_iosxe.17.06.01.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
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

Image added. Version: 17.06.01.0.276
install_add_activate_commit: Activating PACKAGE

gzip: initramfs.cpio.gz: decompression OK, trailing garbage ignored
Following packages shall be activated:
/flash/cat9k_lite-webui.17.06.01.SPA.pkg
/flash/cat9k_lite-srdriver.17.06.01.SPA.pkg
/flash/cat9k_lite-rpboot.17.06.01.SPA.pkg
/flash/cat9k_lite-rpbase.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 all members
Jul 19 13:03:24.337: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds
  [1] Activate package(s) on switch 1
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k_lite-rpbase.17.05.01.SPA.pkg
      Removed cat9k_lite-rpboot.17.05.01.SPA.pkg
      Removed cat9k_lite-srdriver.17.05.01.SPA.pkg
      Removed cat9k_lite-webui.17.05.01.SPA.pkg
    New files list:
      Added cat9k_lite-rpbase.17.06.01.SPA.pkg
      Added cat9k_lite-rpboot.17.06.01.SPA.pkg
      Added cat9k_lite-srdriver.17.06.01.SPA.pkg
      Added cat9k_lite-webui.17.06.01.SPA.pkg
    Finished list of software package changes
  [1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate
```

```
*Jul 19 13:03:24.298 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds--- Starting Commit ---
Performing Commit on all members
  [1] Commit package(s) on switch 1
  [1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Mon Jul 19 13:04:23 IST 2021
Jul 19 13:04:24.586: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE flash:cat9k_lite_iosxe.17.06.01.SPA.bin
```

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

Step 5 Verify installation

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

a) **dir flash:*.pkg**

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

```
Switch# dir flash:*.pkg

Directory of flash:/*.pkg
Directory of flash:/
48582  -rw- 298787860  Mar 20 2021 05:13:32 +00:00  cat9k_lite-rpbase.17.05.01.SPA.pkg
48585  -rw- 35713901   Mar 20 2021 05:14:12 +00:00  cat9k_lite-rpboot.17.05.01.SPA.pkg
48583  -rw- 4252692    Mar 20 2021 05:13:33 +00:00  cat9k_lite-srdriver.17.05.01.SPA.pkg
48584  -rw- 8119312    Mar 20 2021 05:13:34 +00:00  cat9k_lite-webui.17.05.01.SPA.pkg

16640  -rw- 301188116   Jul 19 2021 05:33:25 +00:00  cat9k_lite-rpbase.17.06.01.SPA.pkg
16647  -rw- 35112025    Jul 19 2021 05:34:06 +00:00  cat9k_lite-rpboot.17.06.01.SPA.pkg
16642  -rw- 4326420    Jul 19 2021 05:33:25 +00:00  cat9k_lite-srdriver.17.06.01.SPA.pkg
16643  -rw- 8328208     Jul 19 2021 05:33:25 +00:00  cat9k_lite-webui.17.06.01.SPA.pkg
```

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

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

- `packages.conf`—the file that has been re-written with the newly installed .pkg files
- `cat9k_lite_iosxe.17.06.01.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 19 2021 05:39:42 +00:00  packages.conf
16634 -rw- 4882  Jul 19 2021 05:34:06 +00:00  cat9k_lite_iosxe.17.06.01.SPA.conf
```

Step 6 Reload and verify version

a) **reload**

Use this command to reload the switch. 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.

```
Switch# reload
```

b) **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_LITE_IOSXE), Version
 17.6.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Mon 19-Jul-21 19:57 by mcpre
<output truncated>
```

Downgrading in Install Mode

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

Before you begin

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

When downgrading from ...	To ...
Cisco IOS XE 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 switch model is introduced is the minimum software version for that model.

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 Mon Jul 19 17:46:18 IST 2021
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
```

```
Cleaning flash:
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat9k_lite-rpbase.17.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.17.06.1.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.17.06.1.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.17.06.1.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

The following files will be deleted:
[switch 1]:
/flash/cat9k_lite_iosxe.17.06.1.SPA.bin

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k_lite_iosxe.17.06.1.SPA.bin ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
  [1] Post_Remove_Cleanup package(s) on switch 1
  [1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup

SUCCESS: install_remove  Mon Jul 19 17:47:20 IST 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_lite_iosxe.17.05.1.SPA.bin flash:

Destination filename [cat9k_lite_iosxe.17.05.1.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_lite_iosxe.17.05.1.SPA.bin...
Loading /cat9k_lite_iosxe.17.05.1.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 508584771 bytes]
508584771 bytes copied in 101.005 secs (5035244 bytes/sec)
```

b) **dir flash:**

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

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

Directory of flash:/

434184 -rw- 508584771 Mon Jul 19 2021 13:35:16 -07:00 cat9k_lite_iosxe.17.05.1.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Set boot variable

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

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

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

b) **no boot manual**

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

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

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show boot**

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

```
Switch# show boot
--------------------------
Switch 3
--------------------------
Current Boot Variables:
BOOT variable = flash:packages.conf;

Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = no
Enable Break = yes
Boot Mode = DEVICE
iPXE Timeout = 0
```

Step 4 Downgrade software image

install add file activate commit

Use this command to install the image.

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

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

```
Switch# install add file flash:cat9k_lite_iosxe.17.05.01.SPA.bin activate commit activate
commit

install_add_activate_commit: START Mon Jul 19 13:17:28 IST 2021
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_lite_iosxe.17.05.01.SPA.bin to the selected switch(es)
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
  [1] Add package(s) on switch 1
  [1] Finished Add on switch 1
```

```
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

Image added. Version: 17.05.01.0.203
install_add_activate_commit: Activating PACKAGE

gzip: initramfs.cpio.gz: decompression OK, trailing garbage ignored
Following packages shall be activated:
/flash/cat9k_lite-webui.17.05.01.SPA.pkg
/flash/cat9k_lite-srdriver.17.05.01.SPA.pkg
/flash/cat9k_lite-rpboot.17.05.01.SPA.pkg
/flash/cat9k_lite-rpbase.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 all members
Jul 19 13:29:31.133: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds

*Jul 19 13:29:31.093 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds  [1] Activate package(s)
 on switch 1
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k_lite-rpbase.17.06.01.SPA.pkg
      Removed cat9k_lite-rpboot.17.06.01.SPA.pkg
      Removed cat9k_lite-srdriver.17.06.01.SPA.pkg
      Removed cat9k_lite-webui.17.06.01.SPA.pkg
    New files list:
      Added cat9k_lite-rpbase.17.05.01.SPA.pkg
      Added cat9k_lite-rpboot.17.05.01.SPA.pkg
      Added cat9k_lite-srdriver.17.05.01.SPA.pkg
      Added cat9k_lite-webui.17.05.01.SPA.pkg
    Finished list of software package changes
  [1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
  [1] Commit package(s) on switch 1
  [1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Send model notification for install_add_activate_commit before reload
Install will reload the system now!
SUCCESS: install_add_activate_commit  Mon Jul 19 13:30:52 IST 2021
Jul 19 13:30:53.573: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE flash:cat9k_lite_iosxe.17.05.01.SPA.bin
Jul 19 13:30:53.573 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE flash:cat9k_lite_iosxe.17.05.01.SPA.bin

switch3#
Chassis 1 reloading, reason - Reload command

*Jul 19 13:30:53.529 IST: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_engine:
 Completed install one-shot PACKAGE flash:cat9k_lite_iosxe.17.05.01.SPA.bin
*Jul 19 13:30:54.526 IST: %STACKMGR-1-RELOAD: Switch 1 R0/0: stack_mgr: Reloading due to
reason Reload command Jul 19 13:30:58.121: %PMAN-5-EXITACTION: F0/0: pvp: Process manager
is exiting: reload fp actionrequested
```

```
Jul 19 13:31:01.303: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes
 exit with reload switch code
```

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

Step 5 Verify version

show version

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

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

The following sample output of the **show version** command displays the Cisco IOS XE 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_LITE_IOSXE), Version
17.5.1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
<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 9200 Series Switches fall under these base or add-on license levels.

Base Licenses

- Network Essentials
- Network Advantage—Includes features available with the Network Essentials license and more.

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 Essentials
- DNA Advantage— Includes features available with the DNA Essentials license and more.

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.

Available Licensing Models and Configuration Information

- Cisco IOS XE Fuji 16.9.2 to Cisco IOS XE Amsterdam 17.3.1: Smart Licensing is the default and the only supported method to manage licenses.

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

- 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.

  In the software configuration guide of the required release (17.3.x onwards), see **System Management → Smart Licensing Using Policy**.

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

License Levels - Usage Guidelines

- The duration or term for which a purchased license is valid:

Smart Licensing Using Policy	Smart Licensing
• Perpetual: There is no expiration date for such a license. • Subscription: The license is valid only until a certain date (for a three, five, or seven year period).	• 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.

- Base licenses (Network Essentials and Network-Advantage) are ordered and fulfilled only with a perpetual or permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a subscription or 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.
- When ordering an add-on license with a base license, note the combinations that are permitted and those that are not permitted:

Table 1: Permitted Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No
Network Advantage	Yes[5]	Yes

[5] You will be able to purchase this combination only at the time of the DNA license renewal and not when you purchase DNA-Essentials the first time.

- 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*.

Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst 9200 Series Switches datasheet at:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html

Limitations and Restrictions

- Control Plane Policing (CoPP)—The **show run** command does not display information about classes configured under `system-cpp policy`, when they are left at default values. Use the **show policy-map system-cpp-policy** or the **show policy-map control-plane** commands in privileged EXEC mode instead.
- Hardware limitations
  - Management Port—You cannot modify the configured port speed, duplex mode and flow control and disable auto-negotiation on the Ethernet Management port (GigabitEthernet0/0). Port speed and duplex mode can only be changed from a peer port.
  - Network Module — When the C9200-NM-4X network module is plugged into the C9200 SKUs of the Cisco Catalyst 9200 Series Switches, the uplink interface remains in down state until the network module is recognized by the switch. The time taken for the switch to recognize the network module is longer in comparison to the time taken by the switch to recognize other interconnected devices.
  - If the 1-meter and 1.5-meter 10-GBase-CX1 cables, which are connected on the 10-G ports of the Catalyst 9200L switches, are connected to the 10-G peer ports of the Catalyst 9200L or Catalyst 9200 switches, the peer device might go into the error-disabled state because of link flapping if the local device is restarted. As a workaround, run the **shut** and **no shut** commands on the error-disabled peer interfaces.
- 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).

- Stacking
  - Stacking is supported on Cisco Catalyst 9200 Series Switches. A switch stack supports up to eight stack members. However, you cannot stack C9200 SKUs with C9200L SKUs

    The supported stacking bandwidth on C9200L SKUs is up to 80Gbps; on C9200 SKUs, this is up to 160Gbps.

  - The C9200-24PB and C9200-48PB switch models can be stacked only with each other and not with other models of the Cisco Catalyst 9200 Series Switches.

  - Auto upgrade for a new member switch is supported only in the install mode.

- TACACS legacy command: Do not configure the legacy **tacacs-server host** command; this command is deprecated. If the software version running on your device is Cisco IOS XE Gibraltar 16.12.2 or a later release, using the legacy command can cause authentication failures. Use the **tacacs server** command in global configuration mode.

- USB Authentication—When you connect a Cisco USB drive to the switch, the switch tries to authenticate the drive against an existing encrypted preshared key. Since the USB drive does not send a key for authentication, the following message is displayed on the console when you enter **password encryption aes** command:

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

- 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.

- Upgrading the software image from Cisco IOS XE Gibraltar 16.12.x to any of the later releases can result in a persistent database operation failure and after which the persistent database cannot be restored.

To avoid the persistent database operation failure, use the **dir bootflash:.dbpersist** command to list all DB persist files and then use **delete bootflash:/.dbpersist/folder_name/file_name** and **bootflash:/.dbpersist/folder_name/file_name.meta** commands to delete individual database and meta files from each persistent database folder.

- The File System Check (fsck) utility is not supported in install mode.
- The DiagMemoryTest GOLD test is not supported on the Catalyst 9200 Series Switches.

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	Description
CSCwc15574	Mgig Cat9200 incrementing FCS-Err/Rcv-Err from 1Gig connection

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.7

Identifier	Description
CSCwh38627	C9200L: Stack switch mgmt port reply unknon mac address
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
CSCwc33606	Quake PSU: i2c Errors on DC PSU on turning the power on/off repeatedly
CSCwd28734	Cat9k memory leak in pubd causes switch reload
CSCwe65441	Non PoE 9200/9200L Devices with ARTXXX pwr supply present in SlotA don't boot aftr switch pwr cycle
CSCwe89814	Unexpected reboot due to FED process heldown with Netflow
CSCwe91069	C9200 Unexpected reload upon removing netflow commands.
CSCwc41288	C9200L - Input Errors on Uplinks using 1G SFP
CSCwe79864	9200: Incorrect Iout, pout and PS fan rpm speeds in show env all CLI
CSCwf68913	C9000: Interface link flapping(down/up) occurs at Active Switch after switchover
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

Identifier	Description
CSCwd56540	Ignore higher fan speed deviations on C9200
CSCwd69448	Duplicate power supply removed/restored message are printed upon OIR

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.4

Identifier	Description
CSCwa76242	Cat 9200L - 10G Link Flaps at intermittent times when peer is maintained as Nexus 9K
CSCwa77415	Switch stack shows wrong neighbor info for stack-ports links
CSCwa85199	High CPU Utilization and memory utilization by Smart Licensing Agent
CSCwa92057	Incorrect behaviour seen when tx / rx removed on 1G UL
CSCwb18702	CISCO-ENTITY-SENSOR-MIB is returning wrong threshold values for thermal sensors

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.3

Identifier	Description
CSCvy10601	C9200L-FAN # reports malfunction and recovers on its own.
CSCvy74900	Unexpected reload in HTTP CORE process
CSCvz51752	Randomly CTS enforcement not happening if multiple Tabs are used from the ISE to push COA
CSCvz53278	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
CSCvz77502	9200l 10G port led not blinking green under speed mode
CSCwa17969	Cat9k | standby unexpected reload when no ip helper-address global is executed
CSCwa23654	Memory leak in Inline Power IOSd process when PoE is used
CSCwa41298	remote switch doesn't detect link down when one rx fiber cable is unplugged on 9200L
CSCwa67012	Error seen when deleting ip igmp snooping querier
CSCwa76242	Cat 9200L - 10G Link Flaps at intermittent times when peer is maintained as Nexus 9K

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.2

Identifier	Description
CSCvy27930	C9200 management port linkup with 1000M/Full
CSCvy86484	EsmCpuCredits doesn't get replinished w/ huge amt of ARP traffic, when static mac on multiple ports
CSCvz18983	Interface with "power inline never" and "speed auto 10 100" disables autonegotiation.
CSCvz44094	C9200L boot up error

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.1

Identifier	Description
CSCvw08075	C9200L: Port remains down/down after repeating connect/disconnect of the cable
CSCvw50091	C9200/9200L: Link up detection delay after bootup

Troubleshooting

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

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

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

Related Documentation

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

All support documentation for Cisco Catalyst 9200 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9200-r-series-switches/tsd-products-support-series-home.html

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

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

Communications, Services, and Additional Information

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

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.