Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-31

Last Modified: 2022-09-22

Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS XE Gibraltar 16.12.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 Gibraltar 16.12.8

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.7

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.6

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.5b

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.5

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.4

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.3a

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.3

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.2

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.1

Hardware Features in Cisco IOS XE Gibraltar 16.12.1

Feature Name	Description and Documentation Link
Cisco SFP Modules for Gigabit Ethernet	• Supported transceiver module product numbers: GLC-SX-MM-RGD, GLC-LX-SM-RGD, and GLC-ZX-SM-RGD • Compatible switch model numbers: All C9200 and C9200L SKUs For information about a module, see the Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.
Cisco 100BASE-X Small Form-Factor Pluggable (SFP) Modules	• Supported transceiver module product number: GLC-GE-100FX • Compatible switch model numbers: C9200L-24PXG-2Y, C9200L-48PXG-2Y For information about a module, see Cisco 100BASE-X Small Form-Factor Pluggable Modules for Fast Ethernet Applications Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Software Features in Cisco IOS XE Gibraltar 16.12.1

Feature Name	Description, Documentation Link, and License Level Information
Autoconf Device Granularity to PID of Cisco Switch	Introduces the **platform type** filter option for class map and parameter map configurations. Use the **map platform-type** command in parameter map filter configuration mode, to set the parameter map attribute and the **match platform-type** command in control class-map filter configuration mode, to evaluate control classes. See Network Management → Configuring Autoconf. (Network Essentials and Network Advantage)
Bluetooth Dongle	Introduces support for external USB Bluetooth dongles. The connected dongle acts as a Bluetooth host and serves as a management port connection on the device. See Interface and Hardware Components → Configuring an External USB Bluetooth Dongle. (Network Essentials)
IPv4 and IPv6: Object Groups for access control lists (ACLs)	Enables you to classify users, devices, or protocols into groups and apply them to ACLs, to create access control policies for these groups. With this feature, you use object groups instead of individual IP addresses, protocols, and ports, which are used in conventional ACLs. It allows multiple access control entries (ACEs), and you can use each ACE to allow or deny an entire group of users the access to a group of servers or services. See Security → Object Groups for ACLs.

Feature Name	Description, Documentation Link, and License Level Information
IPv6-based Posture Validation	IPv6 support is introduced for Posture Validation. (Network Advantage and Network Essentials)
Programmability • Zero-Touch Provisioning (ZTP) • GuestShell (On Box Python) • Model-Driven Telemetry gNMI Dial-In • NETCONF-YANG SSH Server Support • YANG Data Models	The following programmability features are introduced in this release: • ZTP—Open Zero Touch Provisioning (ZTP) interface to allow devices to be provisioned and configured automatically, eliminating most of the manual labor involved with adding them to a network. This feature is supported on C9200 SKUs and not on c9200L SKUs. • Guest Shell—A secure LXC container that is an embedded Linux environment and enables you to develop and run Linux and custom Python applications for automated control and management of Cisco switches. Guest Shell is bundled with the software image and can be installed using the guestshell enable command. This feature is supported on C9200 SKUs and not on C9200L SKUs. • Model-Driven Telemetry gNMI Dial-In—Support for telemetry subscriptions and updates over a gRPC Network Management Interface (gNMI). • NETCONF-YANG SSH Server Support—NETCONF-YANG supporting the use of IOS Secure Shell (SSH) public keys (RSA) to authenticate users as an alternative to password-based authentication. • 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/16121. Some of the models introduced in this release are not backward compatible. For the complete list, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16121/BIC. Revision statements embedded in the YANG files indicate if there has been a model revision. The *README.md* file in the same GitHub location highlights changes that have been made in the release. See Programmability. (Network Essentials and Network Advantage)
Software Maintenance Upgrade (SMU)	An SMU is a package that can be installed on a system to provide a fix or a security resolution to a released image. Support for this feature is introduced on the C9200 models of the series. **Note** SMUs require a cold (complete) reload of the operating system; hot patching is not supported on this platform. See System Management → Software Maintenance Upgrade. (DNA Advantage)
Simplified Factory Reset for Removable Storage	Performing a factory reset now also erases the contents of removable storage devices such as Serial Advanced Technology Attachment (SATA), Solid State Drive (SSD), and USB. See System Management → Performing Factory Reset. (Network Advantage)

New on the Web UI	
• 802.1X Port-Based Authentication	Use the WebUI for: • 802.1X Port-Based Authentication—Supports IEEE 802.1X authentication configuration at the interface level. This type of access control and authentication protocol restricts unauthorized clients from connecting to a LAN through publicly accessible ports

Important Notes

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

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
- 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)
- 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://www.cisco.com/go/cfn.

Accessing Hidden Commands

This section provides information about hidden commands in Cisco IOS XE and the security measures in place, when they are accessed. Hidden commands are meant to assist Cisco TAC in advanced troubleshooting and are therefore not documented. For more information about CLI help, see the *Using the Command-Line Interface → Understanding the Help System* chapter of the Command Reference document.

Hidden commands are available under:

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

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

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

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

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

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

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



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

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

Default Behaviour

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

Supported Hardware

Cisco Catalyst 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*.

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

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
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.

Catalyst 9200	Cisco Identity Services Engine	Cisco Prime Infrastructure
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**.
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**.

Catalyst 9200	Cisco Identity Services Engine	Cisco Prime Infrastructure
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[1]	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.

[1] 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[2]	512 MB[3]	256	1280 x 800 or higher	Small

[2] We recommend 1 GHz
[3] 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)

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 Gibraltar 16.12.8	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.12.08.SPA
Cisco IOS XE Gibraltar 16.12.7	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.12.07.SPA
Cisco IOS XE Gibraltar 16.12.6	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.12.06.SPA
Cisco IOS XE Gibraltar 16.12.5b	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.12.05b.SP
Cisco IOS XE Gibraltar 16.12.5	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.12.05.SPA
Cisco IOS XE Gibraltar 16.12.4	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.12.04.SPA
Cisco IOS XE Gibraltar 16.12.3a	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.12.03a.SP
Cisco IOS XE Gibraltar 16.12.3	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.12.03.SPA
Cisco IOS XE Gibraltar 16.12.2	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.12.02.SPA

Release	Image Type	File Name
Cisco IOS XE Gibraltar 16.12.1	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.12.01.S

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.

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE Gibraltar 16.12.2 or Cisco IOS XE Gibraltar 16.12.3 or Cisco IOS XE Gibraltar 16.12.3a or Cisco IOS XE Gibraltar 16.12.4 or Cisco IOS XE Gibraltar 16.12.5 or Cisco IOS XE Gibraltar 16.12.5b or Cisco IOS XE Gibraltar 16.12.6 or Cisco IOS XE Gibraltar 16.12.7 or Gibraltar 16.12.8 the first time	The boot loader may be upgraded to version 16.12.1r [FC7]. For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 16.12.1r [FC7], RELEASE SOFTWARE(P)`

If you boot Cisco IOS XE Gibraltar 16.12.1 the first time	The boot loader may be upgraded to version 16.12.1r. For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 16.12.1r [FC1], RELEASE SOFTWARE(P)`

Software Installation Commands

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

Summary of Software Installation Commands	
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Upgrading in Install Mode

Follow these instructions to upgrade from one release to another, 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 Fuji 16.9.2 and later	Cisco IOS XE Gibraltar 16.12.x

The sample output in this section displays upgrade from Cisco IOS XE Fuji 16.9.2 to Cisco IOS XE Gibraltar 16.12.1 using **install** commands.

Procedure

Step 1 Clean Up

a) **install remove inactive**

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

```
Switch# install remove inactive
install_remove: START Wed Jul 24 17:46:18 IST 2019
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.16.09.02.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.16.09.02.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.16.09.02.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.16.09.02.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.16.09.02.SPA.bin

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

```
[switch 1]:
Deleting file flash:cat9k_lite_iosxe.16.09.02.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  Wed Jul 24 17:47:20 IST 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat9k_lite_iosxe.16.12.01.SPA.bin flash:

Destination filename [cat9k_lite_iosxe.16.12.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_lite_iosxe.16.12.01.SPA.bin...
Loading /cat9k_lite_iosxe.16.12.01.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 24 2019 10:18:11 -07:00 cat9k_lite_iosxe.16.12.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

Step 3 Set boot variable

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

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

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

b) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

c) **show boot system**

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

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

```
Switch# show boot system
```

Step 4 Software install image to flash

a) **install add file activate commit**

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

```
Switch# install add file flash:cat9k_lite_iosxe.16.12.01.SPA.bin activate commit
install_add_activate_commit: START Wed Jul 24 17:32:18 IST 2019

*Jul 24 17:32:21.642 IST: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
 Started install one-shot
flash:cat9k_lite_iosxe.16.12.01.SPA.bininstall_add_activate_commit: Adding PACKAGE

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

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_lite_iosxe.16.12.01.SPA.bin to the selected switch(es)
Finished initial file syncing

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

Image added. Version: 16.12.1.0.214
install_add_activate_commit: Activating PACKAGE

gzip: initramfs.cpio.gz: decompression OK, trailing garbage ignored
Following packages shall be activated:
/flash/cat9k_lite-webui.16.12.01.SPA.pkg
/flash/cat9k_lite-srdriver.16.12.01.SPA.pkg
/flash/cat9k_lite-rpboot.16.12.01.SPA.pkg
/flash/cat9k_lite-rpbase.16.12.01.SPA.pkg

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

--- Starting Commit ---
Performing Commit on all members

*Jul 24 17:36:43.102 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7199 seconds  [1] Commit
package(s) on switch 1
  [1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Wed Jul 24 17:37:03 IST 2019
```

Note

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

b) **dir flash:**

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

```
Switch# dir flash:*.pkg

Directory of flash:/*.pkg
Directory of flash:/

48582  -rw- 298787860 Jul 24 2019 05:13:32 +00:00  cat9k_lite-rpbase.16.09.02.SPA.pkg
48585  -rw- 35713901  Jul 24 2019 05:14:12 +00:00  cat9k_lite-rpboot.16.09.02.SPA.pkg
48583  -rw- 4252692   Jul 24 2019 05:13:33 +00:00  cat9k_lite-srdriver.16.09.02.SPA.pkg
48584  -rw- 8119312   Jul 24 2019 05:13:34 +00:00  cat9k_lite-webui.16.09.02.SPA.pkg

16640  -rw- 301188116 Jul 24 2019 05:33:25 +00:00  cat9k_lite-rpbase.16.12.01.SPA.pkg
16647  -rw- 35112025  Jul 24 2019 05:34:06 +00:00  cat9k_lite-rpboot.16.12.01.SPA.pkg
16642  -rw- 4326420   Jul 24 2019 05:33:25 +00:00  cat9k_lite-srdriver.16.12.01.SPA.pkg
16643  -rw- 8328208   Jul 24 2019 05:33:25 +00:00  cat9k_lite-webui.16.12.01.SPA.pkg
```

The following sample output displays the .conf files in the flash partition; note the two .conf files:

- `packages.conf`—the file that has been re-written with the newly installed .pkg files
- `cat9k_lite_iosxe.16.12.01.SPA.conf`— a backup copy of the newly installed packages.conf file

```
Switch# dir flash:*.conf

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

16631 -rw- 4882  Jul 24 2019 05:39:42 +00:00  packages.conf
16634 -rw- 4882  Jul 24 2019 05:34:06 +00:00  cat9k_lite_iosxe.16.12.01.SPA.conf
```

Step 5 Reload

a) **boot flash:**

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

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

b) **show version**

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

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

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

```
Switch# show version
Cisco IOS XE Software, Version 16.12.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version
 16.12.1, RELEASE SOFTWARE (fc3)
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Tue 24-Jul-19 10:15 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 Gibraltar 16.12.x	Cisco IOS XE Gibraltar 16.11.x or earlier releases.

The sample output in this section shows downgrade from Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Fuji 16.9.2, using **install** commands.



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

Procedure

Step 1 Clean Up

a) **install remove inactive**

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

```
Switch# install remove inactive
install_remove: START Wed Jul 24 17:46:18 IST 2019
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.16.12.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.16.12.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.16.12.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.16.12.01.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.16.12.01.SPA.bin

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k_lite_iosxe.16.12.01.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  Wed Jul 24 17:47:20 IST 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat9k_lite_iosxe.16.09.02.SPA.bin flash:

Destination filename [cat9k_lite_iosxe.16.09.02.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_lite_iosxe.16.09.02.SPA.bin...
Loading /cat9k_lite_iosxe.16.09.02.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 Wed Jul 24 2019 13:35:16 -07:00 cat9k_lite_iosxe.16.09.02.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Downgrade software image

a) **install add file activate commit**

The following example displays the installation of the Cisco IOS XE Fuji 16.9.2 software image to flash, by using the **install add file activate commit** command. You can point to the source image on your tftp server or in flash if you have it copied to flash.

```
Switch# install add file flash:cat9k_lite_iosxe.16.09.02.SPA.bin activate commit
install_add_activate_commit: START Wed Jul 24 17:32:18 IST 2019

*Mar  6 17:32:21.642 IST: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
Started install one-shot flash:cat9k_lite_iosxe.16.09.02.SPA.bin install_add_activate_commit:
```

```
 Adding PACKAGE

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

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_lite_iosxe.16.09.02.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: 16.9.2.0.214
install_add_activate_commit: Activating PACKAGE

gzip: initramfs.cpio.gz: decompression OK, trailing garbage ignored
Following packages shall be activated:
/flash/cat9k_lite-webui.16.09.02.SPA.pkg
/flash/cat9k_lite-srdriver.16.09.02.SPA.pkg
/flash/cat9k_lite-rpboot.16.09.02.SPA.pkg
/flash/cat9k_lite-rpbase.16.09.02.SPA.pkg

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

--- Starting Commit ---
Performing Commit on all members

*Mar  6 17:36:43.102 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7199 seconds  [1] Commit package(s)
 on switch 1
  [1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Wed Jul 24 17:37:03 IST 2019
```

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

Step 4 Reload

a) **boot flash:**

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

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

Note
When you downgrade the software image, the boot loader does not automatically downgrade. It remains updated.

b) **show version**

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

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

The following sample output of the **show version** command displays the Cisco IOS XE Fuji 16.9.2 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.09.02
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 16.9.2,
 RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 24-Jul-19 18:14 by mcpre
```

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.

License Types

The following license types are available:

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

License Levels - Usage Guidelines

- Base licenses (Network Essentials and Network-Advantage) are ordered and fulfilled only with a permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a term license type.
- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- 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[4]	Yes

[4] 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*.

Cisco Smart Licensing

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

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- Unified Management: Cisco License Central provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.

- License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco License Central. For a more detailed overview on Cisco Licensing, visit the Licensing Hub.



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

Deploying Smart Licensing

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

Procedure

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

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

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

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

Step 3 Complete the Cisco Smart Software Manager set up.

a) Accept the Smart Software Licensing Agreement.

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

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

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

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

With this,

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

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

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

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

Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst 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 downlink 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%.
  - Policing and marking policy on sub interfaces is supported.
  - Marking policy on switched virtual interfaces (SVI) is supported.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.
- Secure Shell (SSH)
  - Use SSH Version 2. SSH Version 1 is not supported.
  - When the device is running SCP and SSH cryptographic operations, expect high CPU until the SCP read process is completed. SCP supports file transfers between hosts on a network and uses SSH for the transfer.

Since SCP and SSH operations are currently not supported on the hardware crypto engine, running encryption and decryption process in software causes high CPU. The SCP and SSH processes can show as much as 40 or 50 percent CPU usage, but they do not cause the device to shutdown.

- 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.
  - 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
  ```

- 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 Gibraltar 16.12.x

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.8

Identifier	Description
CSCwa68343	Cisco IOS XE Software for Catalyst Switches MPLS Denial of Service Vulnerability

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.7

Identifier	Description
CSCvu01190	Process install_engine consumes 100% of 1 core after upgrade via DNAC on Cat9K Switches
CSCvz18983	Interface with "power inline never" and "speed auto 10 100" disables autonegotiation.
CSCvz54607	C9200/C9200L (16.12) - Output queue overloaded due to incorrect QoS programming.

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.6

Identifier	Description
CSCvv27849	Cat 9K & 3K: Unexpected reload caused by the FED process.
CSCvw41656	C9200-NM-4X Uplink Module installed in a C9200 is not recognized
CSCvx94722	Radius protocol generate jumbo frames for dot1x packets
CSCvy25845	SNMP: ifHCInOctets - snmpwalk on sub-interface octet counter does not increase

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.5b

Identifier	Description
CSCvr73771	Session not getting authenticated via MAB after shut/no shut of interface
CSCvv27849	Cat 9K & 3K fed crash when running 16.12.5
CSCvw64798	Cisco IOx for IOS XE Software Command Injection Vulnerability

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.5

Identifier	Description
CSCvt52439	C9200 - Some downlink ports did not link up after multiple reload

Identifier	Description
CSCvu62273	CLI should be auto-upgraded from "tacacs-server" cli to newer version while upgrading
CSCvu71598	C9200-48P-E STP block port led display unusual
CSCvv16874	Catalyst Switch: SISF Crash due to a memory leak
CSCvw06037	When "speed nonegotiate" is configured 1G link does not come up after OIR
CSCvw08075	C9200L: Port remains down/down after repeating connect/disconnect of the cable
CSCvw63161	ZTP failing with error in creating downloaded_script.py

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.4

Identifier	Description
CSCvr41932	17.1.1 - Memory leak @ SAMsgThread.
CSCvs71084	Cat9k - Not able to apply Et-analytics on an interface
CSCvs73383	"show mac address-table" does not show remote EIDs when vlan filter used
CSCvs75010	Traffic forwarding stops when Session Idle time out is configured 10 sec with active traffic running
CSCvs77781	Critical auth failing to apply DEFAULT_CRITICAL_DATA_TEMPLATE
CSCvs91195	Crash Due to AutoSmart Port Macros
CSCvs91593	offer is dropped in data vlan with dhcp snooping using dot1x/mab
CSCvs97551	Unable to use VLAN range 4084-4095 for any business operations
CSCvt01187	Eigrp neighbor down up occurred frequently
CSCvt18376	Cat9200: Not able to export control-plane captures to pcap format
CSCvt22238	C9200L/C9200 : Interface counter/MAC learning/MAC ageing does not work/ 32 prefix stuck
CSCvt29004	EHSA keepalive timeout on Active and standby doesn't take over
CSCvt30243	connectivity issue after moving client from dot1x enable port to non dot1x port
CSCvt72427	Cat3k/9k Switch running 16.12.3 is not processing superior BPDUs for non-default native vlan
CSCvt83025	Memory utilization increasing under fman_fp_image due to WRC Stats Req
CSCvt88722	cat9k keep auto-neg enabled even with hard code speed and duplex causing auto-neg mismatch

Identifier	Description
CSCvu03328	SISF-3-INTERNAL: Internal error is seen when MAC move happens and max entry limit is reached
CSCvu04483	Downlink interface on C9200L may remain in looped back state after bootup
CSCvu15007	Crash when invalid input interrupts a role-based access-list policy installation
CSCvu21250	Interfaces won't come up after OIR when using the NM c9200-nm-4x
CSCvs46644	Switches connected to each other are not able to link up when using the same interface ID on both sides

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.3a

Identifier	Description
CSCvt22238	C9200L/C9200 : Interface counter/MAC learning/MAC ageing does not work/ 32 prefix stuck
CSCvt41134	Unexpected reload (or boot loop) caused by Smart Agent (SASRcvWQWrk2)
CSCvt72427	Switch running 16.12.3 is not processing superior BPDUs for non-default native vlan

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.3

Identifier	Description
CSCvm55401	DHCP snooping may drop dhcp option82 packets w/ ip dhcp snooping information option allow-untrusted
CSCvp73666	DNA - LAN Automation doesn't configure link between Peer Device and PnP Agent due CDP limitation
CSCvq19871	RX traffic get stuck on of interface phy ASIC
CSCvq72472	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvr23358	Switches are adding Device SGT to proxy generated IGMP leave messages while keeping End host src IP
CSCvr90477	Cat3k/Cat9k incorrectly set more-fragment flag for double fragmentation
CSCvr91162	Layer 2 flooding floods IGMP queries causing network outage
CSCvr92638	OSPF External Type-1 Route Present in OSPF Database but not in RIB
CSCvs01943	"login authentication VTY_authen" is missing on "line vty 0 4" only
CSCvs14374	Standby crashes on multiple port flaps

Identifier	Description
CSCvs14893	802.1x-MultiAuth/MultiDomain: C9K - Traffic drop in egress direction for Data-Vlan on a Auth port
CSCvs14920	Block overrun crash due to Corrupted redzone
CSCvs15485	Cat9k PoE models - when configuring speed 100 and duplex full on both sides, interface won't come up
CSCvs20038	qos softmax setting doesn't take effect on Catalyst switch in Openflow mode
CSCvs25412	CTS Environmental Data download request triggered before PAC provisioned
CSCvs25428	Netconf incorrectly activate IPv4 address-family for IPv6 BGP peer.
CSCvs36803	When port security applied mac address not learned on hardware
CSCvs42476	Crash during authentication failure of client
CSCvs45231	Memory exhaustion in sessmgrd process due to EAPoL announcement
CSCvs50391	FED crash when premature free of SG element
CSCvs50868	Fed memory leak in 16.9.X related to netflow
CSCvs54360	On Cat9200 and Cat9200L, left PS slot shows Power Supply B
CSCvs61571	Cat3k/Cat9k- OBJ_DWNLD_TO_DP_FAILED after exceeding hardware capacity for adjacency table
CSCvs62003	In COPP policy, ARP traffic should be classified under the "system-cpp-police-forus" class
CSCvs68255	Traceback seen when IS-IS crosses LSP boundary and tries to add information in new LSP
CSCvs73580	Memory leak in fed main event qos
CSCvt00402	cat3k Switch with 1.6GB flash size unable to do SWIM upgrade between 16.12.x images

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.2

Identifier	Description
CSCvq54265	Ip bootp server should be disabled by default as a device hardening best practice.
CSCvr02957	Re-add app-hosting move support was removed.
CSCvr70470	sessmgrd crash with "clear dot1x mac" command
CSCvr57446	Switch crashed at ./VIEW_ROOT/cisco.comp/mka/src/cli/mka_ios_util_defs.c

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.1

Identifier	Description
CSCvn72251	Interface counters/Mac learning does not work after diagnostic test in 9200 and 9200L
CSCvo15594	Hardware MAC address programming issue for remote client catalyst 9300
CSCvo17778	Cat9k not updating checksum after DSCP change
CSCvo24073	multiple CTS sessions stuck in HELD/SAP_NE
CSCvo32446	High CPU Due To Looped Packet and/or Unicast DHCP ACK Dropped
CSCvo62414	C9300, C9200, C9200L switches are unable to stack, one switch stuck in Initializing
CSCvo75559	Cat9300 | First packet not forwarded when (S,G) needs to be built
CSCvp49586	AMBER LED LIGHTS ON WORKING FAN MODULES
CSCvp72220	crash at sisf_show_counters after entering show device-tracking counters command
CSCvp81719	Interface still providing PoE after Port-Security Violation (Err-disable)
CSCvp89233	C9200L- LEDs on few ports not working/bright but traffic passes through fine, reload might recover
CSCvq27812	Sessmgr CPU is going high due to DB cursor is not disabled after switchover
CSCvq56135	C9200 stack member switches reset with reset reason as stack merge

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 results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

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

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

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

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

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

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

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

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

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

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

© 2019–2021 Cisco Systems, Inc. All rights reserved.