Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS XE Fuji 16.9.x

First Published: 2018-11-30

Last Modified: 2021-09-01

Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS XE Fuji 16.9.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.

These switches provide enhanced application visibility, full Layer 2, advanced routing, and enhanced security features that protect the integrity of the hardware as well as software, and all the data that flows through the switch. It provides resiliency that keeps your business up and running seamlessly. Combining this with open APIs of Cisco IOS XE and programmability of the UADP ASIC technology, gives you what you need now with investment protection on future innovations.

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

Whats New in Cisco IOS XE Fuji 16.9.8

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 22.

Whats New in Cisco IOS XE Fuji 16.9.7

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 22.

Software Features in Cisco IOS XE Fuji 16.9.7

Feature Name	Description and License Level Information
Software Maintenance Upgrade (SMU)	The SMU feature is now available with the Network Advantage license. See System Management → Software Maintenance Upgrade. (Network Advantage)

Whats New in Cisco IOS XE Fuji 16.9.6

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 22.

Whats New in Cisco IOS XE Fuji 16.9.5

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 22.

Whats New in Cisco IOS XE Fuji 16.9.4

Software Features in Cisco IOS XE Fuji 16.9.4

Feature Name	Description and License Level Information
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 C9200L 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)

Whats New in Cisco IOS XE Fuji 16.9.3

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 22.

Whats New in Cisco IOS XE Fuji 16.9.2

For the complete list of features available in this introductory release of the platform, see the Cisco Feature Navigator at https://www.cisco.com/go/cfn.

Important Notes

- Unsupported Features, on page 3
- Complete List of Supported Features, on page 4
- Accessing Hidden Commands, on page 4

Unsupported Features

- Audio Video Bridging (including IEEE802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav)
- Bluetooth
- 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
- DNA Service for Bonjour
- Fabric Enabled Wireless
- 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)
- Next Generation NBAR (NBAR2)
- Non Stop Forwarding (NSF)
- Performance Monitoring (PerfMon)
- Programmability (Cisco Plug-in for OpenFlow 1.3, Third-Party Application Hosting, Guest Shell)
- TDR Cable Diagnostics
- 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

Hidden commands have always been present in Cisco IOS XE, but were not equipped with CLI help. This means that entering enter a question mark (?) at the system prompt did not display the list of available commands. Such hidden commands are only 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 Comman 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.

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*.

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
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 Fuji 16.9.8	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.09.08.S
Cisco IOS XE Fuji 16.9.7	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.09.07.S
Cisco IOS XE Fuji 16.9.6	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.09.06.S
Cisco IOS XE Fuji 16.9.5	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.09.05.S
Cisco IOS XE Fuji 16.9.4	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.09.04.S
Cisco IOS XE Fuji 16.9.3	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.09.03.S
Cisco IOS XE Fuji 16.9.2	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.09.02.S

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.

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	Cisco IOS XE Fuji 16.9.x

The sample output in this section displays upgrade from Cisco IOS XE Fuji 16.9.2 to Cisco IOS XE Fuji 16.9.3 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 Fri Mar 22 05:26:37 UTC 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.16.09.03.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.16.09.03.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.16.09.03.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.16.09.03.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

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.16.09.03.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.16.09.03.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.16.09.03.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.16.09.03.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-rpbase.16.09.02.SPA.pkg
/flash/cat9k_lite-rpboot.16.09.02.SPA.pkg
/flash/cat9k_lite-srdriver.16.09.02.SPA.pkg
/flash/cat9k_lite-webui.16.09.02.SPA.pkg
/flash/cat9k_lite_iosxe.16.09.03.SPA.bin
/flash/cat9k_lite_iosxe.16.09.03.SPA.conf
[switch 2]:
/flash/cat9k_lite-rpbase.16.09.02.SPA.pkg
/flash/cat9k_lite-rpboot.16.09.02.SPA.pkg
/flash/cat9k_lite-srdriver.16.09.02.SPA.pkg
/flash/cat9k_lite-webui.16.09.02.SPA.pkg
/flash/cat9k_lite_iosxe.16.09.03.SPA.bin
/flash/cat9k_lite_iosxe.16.09.03.SPA.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k_lite-rpbase.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k_lite-rpboot.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k_lite-srdriver.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k_lite-webui.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k_lite_iosxe.16.09.03.SPA.bin ... done.
Deleting file flash:cat9k_lite_iosxe.16.09.03.SPA.conf ... done.
SUCCESS: Files deleted.
[switch 2]:
Deleting file flash:cat9k_lite-rpbase.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k_lite-rpboot.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k_lite-srdriver.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k_lite-webui.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k_lite_iosxe.16.09.03.SPA.bin ... done.
Deleting file flash:cat9k_lite_iosxe.16.09.03.SPA.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
```

```
Performing Post_Remove_Cleanup on all members
  [1] Post_Remove_Cleanup package(s) on switch 1
  [1] Finished Post_Remove_Cleanup on switch 1
  [2] Post_Remove_Cleanup package(s) on switch 2
  [2] Finished Post_Remove_Cleanup on switch 2
Checking status of Post_Remove_Cleanup on [1 2]
Post_Remove_Cleanup: Passed on [1 2]
Finished Post_Remove_Cleanup

SUCCESS: install_remove  Fri Mar 22 05:28:38 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.106.30.215/cat9k_lite_iosxe.16.09.03.SPA.bin flash:
Address or name of remote host []? 10.106.30.215
Source filename []? cat9k_lite_iosxe.16.09.03.SPA.bin
Destination filename [cat9k_lite_iosxe.16.09.03.SPA.bin]?
Accessing tftp://10.106.30.215/cat9k_lite_iosxe.16.09.03.SPA.bin...
Loading cat9k_lite_iosxe.16.09.03.SPA.bin from 10.106.30.215 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 344552977 bytes]

344552977 bytes copied in 44.604 secs (7724710 bytes/sec)
Switch#
```

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:/

16408  -rw-   344552977  Mar 22 2019 04:48:58 +00:00  cat9k_lite_iosxe.16.09.03.SPA.bin
1956839424 bytes total (1041113088 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** and the manual boot variable is set to **no**.

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.16.09.03.SPA.bin activate commit
install_add_activate_commit: START Fri Mar 22 05:04:34 UTC 2019

*Mar 22 05:04:36.344: %INSTALL-5-INSTALL_START_INFO: Switch 2 R0/0: install_engine:
Started install one-shot
flash:cat9k_lite_iosxe.16.09.03.SPA.bininstall_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
[2]: Copying flash:cat9k_lite_iosxe.16.09.03.SPA.bin from switch 2 to switch 1
[1]: Finished copying to switch 1
Info: Finished copying flash:cat9k_lite_iosxe.16.09.03.SPA.bin to the selected switch(es)
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
  [1] Add package(s) on switch 1
  [1] Finished Add on switch 1
  [2] Add package(s) on switch 2
  [2] Finished Add on switch 2
Checking status of Add on [1 2]
Add: Passed on [1 2]
Finished Add

install_add_activate_commit: Activating PACKAGE

gzip: initramfs.cpio.gz: decompression OK, trailing garbage ignored
Following packages shall be activated:
/flash/cat9k_lite-webui.16.09.03.SPA.pkg
/flash/cat9k_lite-srdriver.16.09.03.SPA.pkg
/flash/cat9k_lite-rpboot.16.09.03.SPA.pkg
/flash/cat9k_lite-rpbase.16.09.03.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

*Mar 22 05:11:12.176: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 2 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.16.09.02.SPA.pkg
      Removed cat9k_lite-rpboot.16.09.02.SPA.pkg
      Removed cat9k_lite-srdriver.16.09.02.SPA.pkg
      Removed cat9k_lite-webui.16.09.02.SPA.pkg
    New files list:
      Added cat9k_lite-rpbase.16.09.03.SPA.pkg
      Added cat9k_lite-rpboot.16.09.03.SPA.pkg
      Added cat9k_lite-srdriver.16.09.03.SPA.pkg
      Added cat9k_lite-webui.16.09.03.SPA.pkg
    Finished list of software package changes
  [1] Finished Activate on switch 1
  [2] Activate package(s) on switch 2
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k_lite-rpbase.16.09.02.SPA.pkg
      Removed cat9k_lite-rpboot.16.09.02.SPA.pkg
      Removed cat9k_lite-srdriver.16.09.02.SPA.pkg
```

```
      Removed cat9k_lite-webui.16.09.02.SPA.pkg
    New files list:
      Added cat9k_lite-rpbase.16.09.03.SPA.pkg
      Added cat9k_lite-rpboot.16.09.03.SPA.pkg
      Added cat9k_lite-srdriver.16.09.03.SPA.pkg
      Added cat9k_lite-webui.16.09.03.SPA.pkg
    Finished list of software package changes
  [2] Finished Activate on switch 2
Checking status of Activate on [1 2]
Activate: Passed on [1 2]
Finished Activate

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

*Mar 22 05:11:13.582: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds  [1] Commit
package(s) on switch 1
  [1] Finished Commit on switch 1
  [2] Commit package(s) on switch 2
  [2] Finished Commit on switch 2
Checking status of Commit on [1 2]
Commit: Passed on [1 2]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Fri Mar 22 05:11:48 UTC 2019
```

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

If you choose to not reload the system by entering **n**, when prompted with the message `This operation requires a reload of the system. Do you want to proceed? [y/n]`, follow the Steps 2 and 3 below to avoid any boot issues during the next or subsequent reloads. You should use these commands only if you chose to not reload the system.

b) **install activate**

Use this command to activate the installed image.

```
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
Install will reload the system now!
SUCCESS: install_activate Fri Mar 22 19:57:48 UTC 2019
```

c) **install commit**

Use this command to commit the installed image. If this step is not performed, the rollback timer takes effect.

```
install_commit: START Thu Jul  10 20:59:43 UTC 2017
Jul  10 20:59:45.556: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 commit
Jul  10 20:59:45.556 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 commit
```

```
install_commit: Committing PACKAGE

--- 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

SUCCESS: install_commit  Fri Mar 22 20:59:52 UTC 2019
```

d) **dir flash:**

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

```
Switch# dir flash:*.conf
```

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.16.09.03.SPA.conf— a copy of packages.conf and not used by the system.

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

Directory of flash:/

56675  -rw-       4877  Mar 22 2019 05:06:34 +00:00  cat9k_lite_iosxe.16.09.03.SPA.conf
16663  -rw-        4877  Mar 22 2019 05:11:00 +00:00  packages.conf
1956839424 bytes total (695914496 bytes free)
```

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 Fuji 16.9.3 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.09.03
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 16.9.3,
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Wed 20-Mar-19 07:19 by mcpre
```

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 Fuji 16.9.5 or Cisco IOS XE Fuji 16.9.4 or Cisco IOS XE Fuji 16.9.3 or Cisco IOS XE Fuji 16.9.2	An earlier release.

The sample output in this section shows downgrade from Cisco IOS XE Fuji 16.9.3 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 Thu Mar 21 17:23:18 UTC 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.16.10.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.16.10.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.16.10.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.16.10.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
```

```
  done.

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.16.10.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.16.10.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.16.10.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.16.10.01.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-rpbase.16.09.03.SPA.pkg
/flash/cat9k_lite-rpboot.16.09.03.SPA.pkg
/flash/cat9k_lite-srdriver.16.09.03.SPA.pkg
/flash/cat9k_lite-webui.16.09.03.SPA.pkg
/flash/cat9k_lite_iosxe.16.10.01.SPA.bin
/flash/cat9k_lite_iosxe.16.10.01.SPA.conf
[switch 2]:
/flash/cat9k_lite-rpbase.16.09.03.SPA.pkg
/flash/cat9k_lite-rpboot.16.09.03.SPA.pkg
/flash/cat9k_lite-srdriver.16.09.03.SPA.pkg
/flash/cat9k_lite-webui.16.09.03.SPA.pkg
/flash/cat9k_lite_iosxe.16.10.01.SPA.bin
/flash/cat9k_lite_iosxe.16.10.01.SPA.conf

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


[switch 1]:
Deleting file flash:cat9k_lite-rpbase.16.09.03.SPA.pkg ... done.
Deleting file flash:cat9k_lite-rpboot.16.09.03.SPA.pkg ... done.
Deleting file flash:cat9k_lite-srdriver.16.09.03.SPA.pkg ... done.
Deleting file flash:cat9k_lite-webui.16.09.03.SPA.pkg ... done.
Deleting file flash:cat9k_lite_iosxe.16.10.01.SPA.bin ... done.
Deleting file flash:cat9k_lite_iosxe.16.10.01.SPA.conf ... done.
SUCCESS: Files deleted.
[switch 2]:
Deleting file flash:cat9k_lite-rpbase.16.09.03.SPA.pkg ... done.
Deleting file flash:cat9k_lite-rpboot.16.09.03.SPA.pkg ... done.
Deleting file flash:cat9k_lite-srdriver.16.09.03.SPA.pkg ... done.
Deleting file flash:cat9k_lite-webui.16.09.03.SPA.pkg ... done.
Deleting file flash:cat9k_lite_iosxe.16.10.01.SPA.bin ... done.
Deleting file flash:cat9k_lite_iosxe.16.10.01.SPA.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
  [1] Post_Remove_Cleanup package(s) on switch 1
  [1] Finished Post_Remove_Cleanup on switch 1
  [2] Post_Remove_Cleanup package(s) on switch 2
  [2] Finished Post_Remove_Cleanup on switch 2
Checking status of Post_Remove_Cleanup on [1 2]
Post_Remove_Cleanup: Passed on [1 2]
Finished Post_Remove_Cleanup
```

```
SUCCESS: install_remove  Thu Mar 21 17:25:12 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.106.30.215/cat9k_lite_iosxe.16.09.03.SPA.bin flash:
Address or name of remote host []? 10.106.30.215
Source filename []? cat9k_lite_iosxe.16.09.03.SPA.bin
Destination filename [cat9k_lite_iosxe.16.09.03.SPA.bin]?
Accessing tftp://10.106.30.215/cat9k_lite_iosxe.16.09.03.SPA.bin...
Loading cat9k_lite_iosxe.16.09.03.SPA.bin from 10.106.30.215 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 344552977 bytes]

344552977 bytes copied in 39.876 secs (8640610 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:/

16408  -rw-   343934509  Mar 21 2019 17:48:03 +00:00  cat9k_lite_iosxe.16.09.02.SPA.bin
1956839424 bytes total (1041137664 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 Thu Mar 21 17:49:14 UTC 2019

*Mar 21 17:49:16.346: %INSTALL-5-INSTALL_START_INFO: Switch 2 R0/0: install_engine: Started
 install one-shot flash:cat9k_lite_iosxe.16.09.02.SPA.bin install_add_activate_commit:
Adding PACKAGE

--- Starting initial file syncing ---
[2]: Copying flash:cat9k_lite_iosxe.16.09.02.SPA.bin from switch 2 to switch 1
[1]: Finished copying to switch 1
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
  [2] Add package(s) on switch 2
  [2] Finished Add on switch 2
Checking status of Add on [1 2]
Add: Passed on [1 2]
Finished Add

install_add_activate_commit: Activating 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
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k_lite-rpbase.16.09.03.SPA.pkg
      Removed cat9k_lite-rpboot.16.09.03.SPA.pkg
      Removed cat9k_lite-srdriver.16.09.03.SPA.pkg
      Removed cat9k_lite-webui.16.09.03.SPA.pkg
    New files list:
      Added cat9k_lite-rpbase.16.09.02.SPA.pkg
      Added cat9k_lite-rpboot.16.09.02.SPA.pkg
      Added cat9k_lite-srdriver.16.09.02.SPA.pkg
      Added cat9k_lite-webui.16.09.02.SPA.pkg
    Finished list of software package changes

*Mar 21 17:54:50.529: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 2 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds
*Mar 21 17:54:51.163: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds  [1] Finished Activate
 on switch 1
  [2] Activate package(s) on switch 2
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k_lite-rpbase.16.09.03.SPA.pkg
      Removed cat9k_lite-rpboot.16.09.03.SPA.pkg
      Removed cat9k_lite-srdriver.16.09.03.SPA.pkg
      Removed cat9k_lite-webui.16.09.03.SPA.pkg
    New files list:
      Added cat9k_lite-rpbase.16.09.02.SPA.pkg
      Added cat9k_lite-rpboot.16.09.02.SPA.pkg
      Added cat9k_lite-srdriver.16.09.02.SPA.pkg
      Added cat9k_lite-webui.16.09.02.SPA.pkg
    Finished list of software package changes
  [2] Finished Activate on switch 2
Checking status of Activate on [1 2]
Activate: Passed on [1 2]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
  [1] Commit package(s) on switch 1
  [1] Finished Commit on switch 1
  [2] Commit package(s) on switch 2
  [2] Finished Commit on switch 2
Checking status of Commit on [1 2]
Commit: Passed on [1 2]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Thu Mar 21 17:55:28 UTC 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 Mon 05-Nov-18 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:
  - Power Supplies — Only the following power supplies are supported. Power supplies other than the following may or may not work properly.
    - PWR-C5-125WAC
    - PWR-C5-600WAC
    - PWR-C5-1KWAC
  - 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.
- 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.

- Stacking:
  - A switch stack supports up to eight stack members.
  - Auto upgrade for a new member switch is supported only in the install mode.

- 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.
- 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 Fuji 16.9.x

Identifier	Description
CSCvn55969	FED crash when 'show tech nbar' is run

Identifier	Description
CSCvr90465	MACSEC link does not recover upon link flap
CSCvs15759	DHCP server sends out a NAK packet during DHCP renewal process.
CSCvv29792	Incorrect Last reload reason shown for scenarios Image upgrade using PnP/Install Cli,Software crash

Resolved Caveats in Cisco IOS XE Fuji 16.9.8

Caveat ID Number	Description
CSCvt53563	Cisco IOS XE Software NETCONF and RESTCONF Authentication Bypass Vulnerability
CSCvt88722	Keep auto-neg enabled even with hard code speed and duplex causing auto-neg mismatch
CSCvu90882	Romvar: Bootloop if SWITCH_DISABLE_PASSWORD_RECOVERY and SWITCH_IGNORE_STARTUP_CFG are both set to 1
CSCvv12527	Crash in SNMP Engine process while polling chassis id in lldp
CSCvw46194	IOS and IOS XE Software UDLD Denial of Service Vulnerability
CSCvx08994	CTS credential password will be added to local keystore even if the password is longer than 24 char
CSCvx34341	Netfilter: Linux Kernel triggers crash by race condition through delete operation
CSCvx41067	IOMD crash when inserting 1G SFP on 25G port
CSCvx41294	High CPU usage caused by "TCP Timer" process
CSCvx55976	Switch stack crash with FIPS mode enabled
CSCvx66699	Cisco IOS and IOS XE Software TrustSec CLI Parser Denial of Service Vulnerability
CSCvy17757	A crash due to issue with internal QOS policy specfic to EPC

Resolved Caveats in Cisco IOS XE Fuji 16.9.7

Caveat ID Number	Description
CSCvn22162	Cat3k crash from corruption in AVL tree
CSCvt30243	connectivity issue after moving client from dot1x enable port to non dot1x port
CSCvu35094	Switch reloads due to fed crash after sending multicast data packets in pvlan
CSCvv48305	Route not fully programmed in the hardware for macsec enabled end-point

Caveat ID Number	Description
CSCvw20578	Switch may reload unexpectedly due to a kernel panic caused by an invalid skb

Resolved Caveats in Cisco IOS XE Fuji 16.9.6

Caveat ID Number	Description
CSCvk03296	"service unsupported-transceiver" command is not working on Cat9200L
CSCvn98703	FED_QOS_ERRMSG-3-POLICER_HW_ERROR on Catalysts switches running 16.6 releases
CSCvr37805	Cat3k/9k: Device might reboot after applying "mac address-static xxxx.xxxx.xxxx vlan x drop" command
CSCvs50391	FED crash when premature free of SG element
CSCvs54360	On Cat9200 and Cat9200L, left PS slot shows Power Supply B
CSCvs69594	%PMAN-3-PROC_EMPTY_EXEC_FILE is output upon system boots up
CSCvs71519	Switch reloads due to dhcp snooping
CSCvs91195	Crash Due to AutoSmart Port Macros
CSCvs91593	offer is dropped in data vlan with dhcp snooping using dot1x/mab
CSCvs93108	POE stops working after upgrading to 16.12.1
CSCvs94235	9200:IQS, SQS shaper configuration for DopplerG based systems
CSCvt02962	Uplink Port-channel Trunk member link Port LED truns to amber blinking after link down/up
CSCvt13518	QoS ACL matching incorrectly when udp range is used
CSCvt29004	EHSA keepalive timeout on Active and standby doesn't take over
CSCvt83025	Memory utilization increasing under fman_fp_image due to WRC Stats Req
CSCvu06092	Cat9200L Hotspot Temperature Value shows 0 on 16.9 Train
CSCvu15007	Crash when invalid input interrupts a role-based access-list policy installation
CSCvu37176	SPAN filter cannot work well when configure FSPAN after 5th session.
CSCvk63813	EFT : "show environment temperature" does not list Outlet Temperature

Resolved Caveats in Cisco IOS XE Fuji 16.9.5

Identifier	Description
CSCvk47894	Cat3k/9k SPAN monitor session works in stack only on adding 2 dest ports in stack

Identifier	Description
CSCvm72574	16.6.4 CPP Police rate wrong in "class system-cpp-police-control-low-priority"
CSCvo81311	FMAN-RP crash observed on Guest Anchor
CSCvp84502	ERSPAN destination does not work or forward traffic
CSCvq22011	IOS-XE drops ARP reply when IPDT gleans from ARP
CSCvq38901	Enable CDP - removed on shut/ no shut dot1Q-tunnel interface
CSCvq44397	Cat3k/9k Ospf down upon switchover with aggressive timers "hello-interval 1" and "dead-interval 4"
CSCvq50846	ip verify source mac-check prevents device tracking from getting arp probe reply
CSCvq55940	%BIT-4-OUTOFRANGE: bit 4095 is not in the expected range of 1 to 4093
CSCvq66802	igmp query with src ip 0.0.0.0 is not ignored
CSCvq68337	Cat3k/9k does not forward packet when active route down
CSCvq72472	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvq72713	Cat3k/Cat9k can't forwarding traffic follow the rule of EIGRP unequal cost load-balancing
CSCvq75887	intermediate hop with SVI in PIM domain is not forwarding multicast traffic
CSCvq94738	The COPP configuration back to the default After rebooting the device
CSCvr03905	Memory Leak on FED due to IPv6 Source Guard
CSCvr04551	Multicast stream flickers on igmp join/leave
CSCvr20522	Cat3k/9k BOOTREPLY dropped when DHCP snooping is enabled
CSCvr23358	Switches are adding Device SGT to proxy generated IGMP leave messages while keeping End host src IP
CSCvr30559	Switch may experience a kernel panic due to invalid skb
CSCvr32460	Cat3k/9k stack breaks and subsequent merge fails
CSCvr46931	ports remain down/down object-manager (fed-ots-mo thread is stuck)
CSCvr48249	High memory utilization under fman_fp_image
CSCvr59959	Cat3k/9k Flow-based SPAN(FSPAN) can only work in one direction when mutilple session configured
CSCvr98281	After valid ip conflict, SVI admin down responds to GARP
CSCvr98368	CAT9K intermittently not responding to SNMP

Identifier	Description
CSCvs50868	Fed memory leak in 16.9.X related to netflow

Resolved Caveats in Cisco IOS XE Fuji 16.9.4

Caveat ID Number	Description
CSCvj15473	Linux IOSD crash with sh vtp counters cmd
CSCvj84601	Called-Station-Id attribute not included in Radius Access-Request
CSCvm80443	IOSd memory leak within DSMIB Server within xqos_malloc_wrapper
CSCvm91107	standby reloads and crashed @fnf_ios_config_dist_validate_sel_process_add
CSCvm91642	MACsec SAP 128 Bits doesn't work with network-essentials license
CSCvn30230	Catalyst 3k/9k: Slow memory leak in linux_iosd-imag
CSCvn57892	High Memory utilization due to Wireless Manager IOSD process
CSCvn69629	ND packets received in remote vtep SISF table - EVPN part
CSCvn99482	IPv6 traffic is stopped on interface when more than 3 invalid ARPs are detected
CSCvo05751	Changes for sending vlan attrs in access request
CSCvo21122	Memory leak at hman process
CSCvo42353	SDA-Cat9k-External border creating incorrect CEF/map-cache entry due to multicast
CSCvo49876	SISF not honoring 1 IPv4-to-MAC rule when DHCP ACK comes from a different VLAN (via Relay)
CSCvo57768	NetFlow issue 3850 switch not sending TCP flags
CSCvo60400	errdisable detect cause bpduguard shutdown vlan continues to forward BPDUs
CSCvo61570	spanning-tree uplinkfast max-update-rate's value is abnormal
CSCvo65974	QinQ tunnels causing L2 loop in specific topology of Cat3850
CSCvo66246	Enabling SPAN source of VLAN 1 affects LACP operations
CSCvo71264	Cat3k / Cat9k Gateway routes DHCP offer incorrectly after DHCP snooping
CSCvo73205	Identity policy won't update after config changes.
CSCvo73897	[SDA] [PI changes] No audio during first few seconds of voice call between 2 Fabric Edge
CSCvo75559	Cat9300 | First packet not forwarded when (S,G) needs to be built
CSCvo78538	Counters in the "show interface" command are not increasing

Caveat ID Number	Description
CSCvo85422	Directly connected IPv4/IPv6 hosts not programmed in HW - %FMFP-3-OBJ_DWNLD_TO_DP_FAILED
CSCvp00026	[SDA] [PD changes] No audio during first few seconds of voice call between 2 Fabric Edge
CSCvp03816	ENH Hex dump constantly logging when registering access point using DNAC
CSCvp09091	When sourcing Radius from loopback in VRF, auth right out of boot up might fail
CSCvp12187	Standby switch crash due to memory leak due to Switch Integrated Security feature
CSCvp13114	Cat9400 incoming packet from PVLAN access port is not forwarded out on etherchannel interface
CSCvp26792	Cat9k control plane impacted when > 1Gbps multicast passes through and no entry in IGMP snooping
CSCvp30629	Cat9300: Lisp site entry count mismatch in external dual border on reload
CSCvp49518	DHCP SNOOPING DATABASE IS NOT REFRESHED AFTER RELOAD
CSCvp54779	[SDA] 1st ARP Reply is dropped at remote Fabric Edge
CSCvp65173	SDA: DHCP offer being dropped on BN with L2 and L3 Handoff configured
CSCvp72220	crash at sisf_show_counters after entering show device-tracking counters command
CSCvp75221	Modules shows faulty status when specific MAC ACL is applied on interfaces
CSCvp81190	%FED_QOS_ERRMSG-3-TABLEMAP_INGRESS_HW_ERROR was generated after setting policy-map with table-map
CSCvp85601	STP TCN is generated on etherchannel port during a switchover in a 3850 stack
CSCvp86983	Connectivity over AC tunnel broken due to tunnel deletion from FMAN FP but remains FMAN FP
CSCvp90279	Catalyst switches is sending ADV and REP DHCPv6 packets to SISF when source udp port is not 547
CSCvq30316	[SDA] 1st ARP fix for CSCvp00026 is eventually failing after longevity
CSCvq30460	SYS-2-BADSHARE: Bad refcount in datagram_done - messages seen during system churn
CSCvq40137	Mac address not being learnt when "auth port-control auto" command is present
CSCvq55779	FIVE GIG INTERFACE NOT SHOWING IN CLI WHILE CONFIGURING IP IGMP SNOOPING

Resolved Caveats in Cisco IOS XE Fuji 16.9.3

Identifier	Description
CSCvm98644	poe power budget comes up as 'n/a' after switch reload in stack
CSCvn30950	16.10.1: c9300 stack could run into a state where all member switch are removed until reboot
CSCvo00968	Radius attr 32 NAS-IDENTIFIIER not sending the FQDN
CSCvo33983	Mcast traffic loss seen looks due to missing fed entries during IGMP/MLD snooping.
CSCvo62414	C9300, C9200, C9200L switches are unable to stack, one switch stuck in Initializing

Resolved Caveats in Cisco IOS XE Fuji 16.9.2

Identifier	Description
CSCvg81784	Converting a layer 2 port-channel to L3 causes some Protocols to break
CSCvj16271	Addressing memory leaks in IPC error handling cases in LED, RPS, VMARGIN, USB, THERMAL
CSCvj66609	DHCP offer received from SVI sent back to the same SVI when DHCP Snooping is enabled
CSCvj75719	System returning incorrect portchannel MIB value (IEEE8023-LAG-MIB)
CSCvk16813	DHCP client traffic dropped with DHCP snooping and port-channel or cross stack uplinks.
CSCvk53444	Packets with Fragment Offset not forwarded with DHCP Snooping Enabled

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.

© 2018–2021 Cisco Systems, Inc. All rights reserved.