Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS XE Gibraltar 16.10.x

First Published: 2018-12-10

Last Modified: 2019-01-24

Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS XE Gibraltar 16.10.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 16.10.1

Hardware Features in Cisco IOS XE Gibraltar 16.10.1

Feature Name	Description and Documentation Link
Cisco Catalyst 9200 Series Switches	New hardware models introduced in this release: • C9200-24T: 24-port data • C9200-24P: 24-port PoE+ • C9200-48T: 48-port data • C9200-48P: 48-port PoE+ For information about the hardware, see the Cisco Catalyst 9200 Series Switches Hardware Installation Guide.
Cisco Catalyst 9200 Series Switches—Network Modules	The following uplink network modules are available with the C9200 SKUs: • C9200-NM-4G—Four ports (1-GigabitEthernet SFP module slots) • C9200-NM-4X for 10G—Four ports (10-GigabitEthernet SFP+ module slots) For information about the hardware, see the Cisco Catalyst 9200 Series Switches Hardware Installation Guide.

Software Features in Cisco IOS XE Gibraltar 16.10.1

(C9200) = C9200-24T, C9200-24P, C9200-48T, C9200-48P

(C9200L) = C9200L-24P-4G, C9200L-24P-4X, C9200L-24T-4G, C9200L-24T-4X, C9200L-48P-4G, C9200L-48P-4X, C9200L-48T-4G, C9200L-48T-4X

Feature Name	Description, Documentation Link and License Level Information
EIGRP BFD (C9200 and C9200L)	Configures the Enhanced Interior Gateway Routing Protocol (EIGRP) with Bidirectional Forwarding Detection (BFD) so that EIGRP registers with BFD and receives all forwarding path detection failure messages from BFD. See Routing → Configuring BFD-EIGRP Support. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link and License Level Information
Media Access Control Security (MACsec): MACsec connection across intermediate switches (C9200 and C9200L)	MACsec connections between end devices in a WAN MACsec deployment with intermediate switches as Catalyst 9000 Series Switches is supported. See Security → MACsec Encryption. 128-bit—(Network Essentials and Network Advantage)
Programmability • Model Driven Telemetry - gRPC Dial-Out • YANG Data Models (C9200 and C9200L)	These programmability features were introduced in the release: • Model Driven Telemetry - gRPC Dial-Out—Expands existing Model Driven Telemetry capabilities with the addition of gRPC protocol support and Dial-Out (configured) telemetry subscriptions. (Network Essentials and Network Advantage) • YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16101. 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 Configuration Guide, Cisco IOS XE Gibraltar 16.10.x.
Secure Shell File Transfer Protocol (SFTP) (C9200 and C9200L)	Secure Shell (SSH) now includes support for SSH File Transfer Protocol (SFTP), a new standard file transfer protocol introduced in SSHv2. This feature provides a secure and authenticated method for copying device configuration or device image files. See Security → Configuring SSH File Transfer Protocol. (Network Essentials and Network Advantage)

Serviceability	
(C9200 and C9200L) See → Command Reference, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9200 Switches).	
debug commands	• The **debug ilpower** command output was enhanced to display the power unit (mW). • The **debug platform software fed switch active punt packet-capture** command was introduced. It enables debugging of packets during high CPU utilization.
show logging commands	The **show logging onboard switch uptime** command ws introduced. It displays a history of all reset reasons for all modules or switches in a system.

Serviceability	
show platform commands	• The **show platform hardware fed switch forward interface** command was enhanced to trace packets across a stack and also trace packets captured in a PCAP file. • The **show platform software fed switch punt rates interfaces** command was introduced. It displays the overall statistics of punt rate for all the interfaces. • The **show platform software fed punt cpuq rates** command was introduced. It displays the rate at which packets are punted, including the drops in the punted path. • The **show platform software fed switch punt packet-capture display** command was introduced. It displays packet information captured during high CPU utilization. • The **show platform integrity** command output was enhanced to display version information for individual packages in the software bundle. • The **show platform software process memory** command was modified and the virtual size column was deleted from the output. • The **show platform software thread list** and **show platform software process list** commands outputs were modified. The `size` columns in the outputs display the Resident Set Size (RSS) in KB.
show processes commands	The **show processes platform**, **show processes cpu platform**, and **show processes cpu platform history** commands outputs were modified. The `size` columns in the outputs display the Resident Set Size (RSS) in KB.
show processes memory platform commands	• **show processes memory platform** command was enhanced, the **accounting** keyword was added. • The **show processes memory platform**, **show processes memory platform location**, and **show processes memory platform sorted** commands were modified and the `Total` column was deleted from the output.

Serviceability	
show tech-support commands	• The **show tech-support** command was modified to display the history of all reset reasons for all modules or switches in a system. • The **show tech-support acl** command was introduced. It displays access control list (ACL)-related information. • The **show tech-support platform** command was introduced. It displays detailed information about a platform. • The **show tech-support platform igmp_snooping** command was introduced. It displays Internet Group Management Protocol (IGMP) snooping information about a group. • The **show tech-support poe** command was introduced. It displays outputs of all the PoE-related troubleshooting commands. • The **show tech-support port** command output was updated. • The **show tech-support qos control-plane** command was introduced. It displays QoS-related information for the control-plane. • The **show tech-support qos** command was introduced. It displays the Quality of Service (QoS)-related information.

New on the Web UI	
Web UI (C9200 and C9200L)	• Spanning Tree Protocol (STP) in Layer 2 configuration—Provides path redundancy to build a loop-free topology for Ethernet networks. Security mechanisms like bridge protocol data units (BPDU) Guard and BPDU Filtering provide further protection by ensuring a more stable network. • VLAN Trunk Protocol (VTP)—Reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere.

Important Notes

• Unsupported Features, on page 5
• Complete List of Supported Features, on page 6
• Accessing Hidden Commands, on page 6

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)
- Time-Domain Reflectometer (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*.

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 16.10.1	2.4	C9200: PI 3.4 + Device Pack 9 C9200L: PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.8	2.5 2.1	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.7	2.5 2.1	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.6	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.5	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.4	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.3	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.2[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 16.10.1	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.16.10.01.SPA

Automatic Boot Loader Upgrade

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

For subsequent Cisco IOS XE Everest 16.x.x, or Cisco IOS XE Fuji 16.x.x releases, if there is a new bootloader in that release, it may be automatically upgraded based on the hardware version of the switch when you boot up your switch with the new image for the first time.

Caution Do not power cycle your switch during the upgrade.

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE Gibraltar 16.10.1 the first time	On Cisco Catalyst 9200 Series Switches, the boot loader may be upgraded to version 16.10.1r [FC4]. For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 16.10.1r [FC4], 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.

Summary of Software Installation Commands	
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.x	Cisco IOS XE Gibraltar 16.10.1

The sample output in this section displays upgrade from Cisco IOS XE Fuji 16.9.2 to Cisco IOS XE Gibraltar 16.10.1 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 Mon Dec  3 17:46:18 IST 2018
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  Mon Dec  3 17:47:20 IST 2018
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.16.10.01.SPA.bin flash:

Destination filename [cat9k_lite_iosxe.16.10.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_lite_iosxe.16.10.01.SPA.bin...
Loading /cat9k_lite_iosxe.16.10.01.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 Oct 31 2018 10:18:11 -07:00 cat9k_lite_iosxe.16.10.01.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.16.10.01.SPA.bin activate commit
install_add_activate_commit: START Mon Dec  3 17:32:18 IST 2018

*Dec  3 17:32:21.642 IST: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
 Started install one-shot
flash:cat9k_lite_iosxe.16.10.01.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.16.10.01.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: 16.10.1.0.214
install_add_activate_commit: Activating PACKAGE

gzip: initramfs.cpio.gz: decompression OK, trailing garbage ignored
Following packages shall be activated:
/flash/cat9k_lite-webui.16.10.01.SPA.pkg
/flash/cat9k_lite-srdriver.16.10.01.SPA.pkg
/flash/cat9k_lite-rpboot.16.10.01.SPA.pkg
/flash/cat9k_lite-rpbase.16.10.01.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

*Dec  3 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  Mon Dec  3 17:37:03 IST 2018
```

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 nine new `.pkg` files and three `.conf` files.

```
Switch# dir flash:

Directory of flash:/
```

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

- packages.conf—the file that has been re-written with the newly installed .pkg files
- packages.conf.00—backup file of the previously installed image
- cat9k_lite_iosxe.16.010.01.SPA.conf— a copy of packages.conf and not used by the system.

```
Switch# dir flash:*.conf

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

434197 -rw- 7406 Dec 03 2018 10:59:16 -07:00 packages.conf
434196 -rw- 7504 Dec 03 2018 10:59:16 -07:00 packages.conf.00-
516098 -rw- 7406 Dec 03 2018 10:58:08 -07:00 cat9k_lite_iosxe.16.10.01.SPA.conf
11353194496 bytes total (8963174400 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 Gibraltar 16.10.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.10.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version
 16.10.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Fri 09-Nov-18 18:29 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 Gibraltar 16.10.1	An earlier release.

The sample output in this section shows downgrade from Cisco IOS XE Gibraltar 16.10.1 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 Mon Dec  3 17:46:18 IST 2018
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_iosxe.16.10.01.SPA.bin

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k_lite_iosxe.16.10.01.SPA.bin ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
  [1] Post_Remove_Cleanup package(s) on switch 1
  [1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup

SUCCESS: install_remove  Mon Dec  3 17:47:20 IST 2018
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 Oct 31 2018 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 Mon Dec  3 17:32:18 IST 2018

*Dec  3 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: 16.10.1.0.214
install_add_activate_commit: Activating PACKAGE

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

*Dec  3 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  Mon Dec  3 17:37:03 IST 2018
```

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.
  - If the 1-meter and 1.5-meter 10-GBase-CX1 cables, which are connected on the 10-G ports of the Catalyst 9200L switches, are connected to the 10-G peer ports of the Catalyst 9200L or Catalyst 9200 switches, the peer device might go into the error-disabled state because of link flapping if the local device is restarted. As a workaround, run the **shut** and **no shut** commands on the error-disabled peer interfaces.
- QoS restrictions
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - For QoS policies, only switched virtual interfaces (SVI) are supported for logical interfaces.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.
- Secure Shell (SSH)

- Use SSH Version 2. SSH Version 1 is not supported.
- When the device is running SCP and SSH cryptographic operations, expect high CPU until the SCP read process is completed. SCP supports file transfers between hosts on a network and uses SSH for the transfer.

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

- 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.

- 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.
- Secure Password Migration—Type 6 encrypted password is supported from Cisco IOS XE Gibraltar 16.10.1 and later releases. Autoconversion to password type 6 is supported from Cisco IOS XE Gibraltar 16.11.1 and later releases.

  If the startup configuration has a type 6 password and you downgrade to a version in which type 6 password is not supported, you can/may be locked out of the device.
- 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 16.10.x

Caveat ID Number	Description
CSCvh85225	Smart licensing(SL)Actions done soon after system bootup can cause SL to get stuck, requiring reload

Resolved Caveats in Cisco IOS XE Gibraltar 16.10.1

There are no resolved caveats in this release.

Troubleshooting

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

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

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

Related Documentation

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

All support documentation for Cisco Catalyst 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 Cisco Systems, Inc. All rights reserved.