Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Fuji 16.8.x

First Published: 2018-04-06

Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Fuji 16.8.x

Introduction

Cisco Catalyst 9400 Series Switches are Cisco's leading modular enterprise switching access platform and has been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

They deliver complete convergence with the rest of the Cisco Catalyst 9000 Series Switches in terms of ASIC architecture with a Unified Access Data Plane (UADP) 2.0. The platform runs an Open Cisco IOS XE that supports model driven programmability, has the capacity to host containers, and run 3rd party applications and scripts natively within the switch (by virtue of x86 CPU architecture, local storage, and a higher memory footprint). The series forms the foundational building block for SD-Access, which is Cisco's lead enterprise architecture.

Cisco Catalyst 9400 Series Switches are enterprise optimized with a dual-serviceable fan tray design, side to side airflow, and are closet-friendly with a16-inch depth

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 16.8.1a

Hardware Features in Cisco IOS XE Fuji 16.8.1a

Feature Name	Description and Documentation Link
Cisco Catalyst 9400 Series Switching Modules (line cards)	• C9400-LC-24S Cisco Catalyst 9400 Series 24 Port, 1-GigabitEthernet SFP module that supports 100/1000 BASE-T with Cu-SFP • C9400-LC-48S Cisco Catalyst 9400 Series 48 Port, 1-GigabitEthernet SFP module that supports 100/1000 BASE-T with Cu-SFP • C9400-LC-48P Cisco Catalyst 9400 Series 48 Port, 1-GigabitEthernet PoE/PoE+ modulethat supports up to 30W per port. For information about the hardware, see Cisco Catalyst 9400 Series Switching Module Installation Note.
Cisco 100-Megabit Ethernet SFP Modules—GLC-GE-100FX	Supported SFP module product number—GLC-GE-100FX For information about the module, see Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix.

PORT SET ENABLED LEDs for SFP or SFP+ ports	These LEDs are now supported and indicate SFP or SFP+ ports that are enabled.
	
	There are two such LEDs on the supervisor module faceplate:
	
	   • One for port numbers 1 to 4.
	
	   • One for port numbers 5 to 8.
	
	The LEDs are solid green when the port set is enabled and off when the port set is not enabled.
	
	For information about the LEDs, see Cisco Catalyst 9400 Series Supervisor Module Installation Note → Cisco Catalyst 9400 Series Supervisor Module LEDs.

Power Supply Module—C9400-PWR-2100AC	Supported power supply modules now include the Cisco Catalyst 9400 Series 2100W AC Input Power Supply Module

Software Features in Cisco IOS XE Fuji 16.8.1a

Feature Name	Description and License Level Information
Auto-Upgrade	Detects and rectifies software version mismatches between a currently active supervisor and a standby supervisor in the chassis. When the system detects a mismatch, it enables the standby supervisor's software version to be automatically synchronised to match the software version of the active supervisor. (Network Advantage)
DHCPv6: Client Link-Layer Address Option (RFC 6939)	Defines an optional mechanism and the related DHCPv6 option to allow first-hop DHCPv6 relay agents (relay agents that are connected to the same link as the client) to provide the client's link-layer address in the DHCPv6 messages being sent towards the server. (Network Essentials and Network Advantage)
DHCPv6: Support for Option 52 and DNS Search List (DNSSL) Option	Wireless access points use the The Dynamic Host Configuration Protocol version 6 (DHCPv6) option 52 (RFC 5417) to supply the IPv6 management interface addresses of the primary, secondary, and tertiary wireless controllers. The DNSSL option is a list of DNS suffix domain names used by IPv6 hosts when they perform DNS query searches for short, unqualified domain names. The DNSSL option contains one or more domain names. (Network Essentials and Network Advantage)
Support for validation of DHCP Option 125	DHCP option 125 is used by DHCP clients and servers to identify vendor-specific information. Support for validation of DHCP option 125 is enabled if the switch is configured as a DHCP relay agent or if the DHCP snooping feature is turned on. Note that the switch drops those packets that do not conform to the RFC3925 format (HEX format) of option 125.

Feature Name	Description and License Level Information
Encrypted Traffic Analytics (ETA)	Studies the packet flow behavior of an application to determine the flow characteristics such as, malware analysis and crypto audit. (DNA Advantage)
High Availability— Graceful Insertion and Removal (GIR)	Uses a maintenance mode to isolate the switch from the network in order to perform debugging, or an upgrade. GIR is supported for Layer 2 interface shutdown and the Intermediate System to Intermediate System (IS-IS) routing protocol. When you place the switch in maintenance mode, supported protocols are isolated, and Layer 2 interfaces are shut down. When normal mode is restored, the supported protocols and ports are brought back up. (Network Advantage)
Hitless ACL Updates (IPv4 and IPv6)	Provides the capability to apply existing features to incoming traffic while updating new features in the TCAM. The feature prevents TCAM reprogramming everytime there is a change in an IPv4 or IPv6 ACL on a given interface. (Network Advantage)
IGMP packet forwarding in IEEE 802.1Q Tunneling	This enhancement enables Internet Group Management Protocol (IGMP) packet forwarding in IEEE 802.1Q tunnels (Network Essentials and Network Advantage)

Feature Name	Description and License Level Information
IPv6 support for IEEE 802.1Q Tunneling	Enables IPv6 support for the existing 802.1Q tunneling feature.
	802.1Q tunneling, also known as Q-in-Q, enables service providers to use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated. A port configured to support 802.1Q tunneling is called a tunnel port. When you configure tunneling, you assign a tunnel port to a VLAN ID that is dedicated to tunneling.
	(Network Essentials and Network Advantage)
OCSP multiple response handling	Enables support to handle multiple Online Certificate Status Protocol (OCSP) single responses on an OCSP client.
	(Network Advantage)

Feature Name	Description and License Level Information
Programmability	

Feature Name	Description and License Level Information
	• Guest Shell Logging and Tracing Support—Provides logging services for guest applications that run separately from the host system, to report tracing data to the host file system. The tracing data is saved in an IOX tracelog and the logging data is saved in the IOS syslog, on the host machine.
	• Model Based AAA—Implements the NETCONF Access Control Model (NACM). NACM is a form of role-based access control (RBAC) specified in RFC 6536.
	• NETCONF Global Session Lock and Kill Session—Provides a global lock and the ability to kill non-responsive sessions in NETCONF. During a session conflict or client misuse of the global lock, NETCONF sessions can be monitored via the **show netconf-yang sessions** command, and non-responsive sessions can be cleared using the clear configuration lock command.
	• NETCONF and RESTCONF Debug commands—Commands for debugging were added.
	• NETCONF and RESTCONF IPv6 Support—Data model interfaces (DMIs) support the use of IPv6 protocol. DMI IPv6 support helps client applications to communicate with services that use IPv6 addresses. External facing interfaces will provide dual-stack support; both IPv4 and IPv6.
	• RESTCONF—Provides an RFC 8040 compliant HTTP-based protocol that provides a programmatic interface for accessing data defined in YANG, using the datastore concepts defined in NETCONF.
	• 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/1681. 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.
	• Operational Data Parser Polling—Starting with

Feature Name	Description and License Level Information
	Cisco IOS XE Fuji 16.8.1a, the Operational Data Parser Polling feature is deprecated. All operational data models provide direct operational data model access, hence this feature is no longer required. (Network Essentials and Network Advantage)
Secure Storage of Encryption Keys and Passwords	Secures critical configuration, keys, and passwords by encrypting them. An instance-unique encryption key is stored in the hardware trust anchor to prevent it from being compromised. This feature is enabled on platforms that come with a hardware trust anchor, by default and is not supported on platforms that do not have a hardware trust anchor. (Network Essentials and Network Advantage)
Simplified Factory Reset	Removes all customer specific data that has been added to the device since the time of its shipping. Data erased includes configurations, logfiles, bootvariables, corefiles, and credentials. (Network Essentials and Network Advantage)
Transmission Control Protocol (TCP) Maximum Segment Size (MSS) Adjustment	Enables configuration of the maximum segment size for transient packets that traverse the device during a TCP session.
Virtual Ethernet Port Aggregator (VEPA)	Also referred to as reflective relay, the feature moves switching out of the server, back to the physical network, and makes all virtual machine traffic visible to the external network switch. This frees up server resources to support virtual machines. VEPA provides several benefits to Virtual Ethernet Bridge (VEB), which is a physical end station capability that supports local bridging between multiple virtual end stations. (Network Essentials and Network Advantage)
VRF-Aware SGACL Logging	Enables logging of a Virtual Routing and Forwarding (VRF) name in Security Group Access Control List (SGACL) logs, making them VRF aware. (DNA Advantage)

New on the Web UI	
These features are introduced on the Web UI in this release	• Python Sandbox—A new sandbox is introduced that to allows you to learn the Python APIs available to execute IOS commands (both Configuration and EXEC CLIs) and NETCONF requests. You can try sample Python scripts to see how the network device responds to them and get a better understanding of how Python APIs operate on the device. You can safely run your Python scripts in the sandbox before applying them to the network device. • Expose the password life time details from AAA to Web UI—A new security mechanism for defining rules, constraints and restrictions when specifying user passwords.

Important Notes

Unsupported Features

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

- Bluetooth

- Cisco Plug-in for OpenFlow 1.3

- Cisco StackWise Virtual

- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks

- Converged Access for Branch Deployments

- Gateway Load Balancing Protocol (GLBP)

- IPsec VPN

- MACSec Encryption

- Network-Powered Lighting (including COAP Proxy Server, 2-event Classification, Perpetual POE, Fast PoE)

- Performance Monitoring (PerfMon)

- Virtual Routing and Forwarding (VRF)-Aware web authentication

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

Starting with Cisco IOS XE Fuji 16.8.1a, as an improved security measure, the way in which hidden commands can be accessed has changed.

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. For information about CLI help, see Understanding the Help System. Such hidden commands are only meant to assist Cisco TAC in advanced troubleshooting and are therefore not documented.

Starting with Cisco IOS XE Fuji 16.8.1a, 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 <u>any</u> 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 9400 Series Switches—Model Numbers

The following table lists the supported switch models. For information about the available license levels, see section *License Levels*.

Switch Model (append with "=" for spares)	Description
C9404R	Cisco Catalyst 9400 Series 4 slot chassis • Redundant supervisor module capability • Two switching module slots • Hot-swappable, front and rear serviceable, non-redundant fan tray assembly • Four power supply module slots
C9407R	Cisco Catalyst 9400 Series 7 slot chassis • Redundant supervisor module capability • Five switching module slots • Hot-swappable, front and rear serviceable fan tray assembly • Eight power supply module slots
C9410R	Cisco Catalyst 9400 Series 10 slot chassis • Redundant supervisor module capability • Eight switching module slots • Hot-swappable, front and rear serviceable fan tray assembly • Eight power supply module slots

Supported Hardware on Cisco Catalyst 9400 Series Switches

Product ID (append with "=" for spares)	Description
Supervisor Modules	
C9400-SUP-1	Cisco Catalyst 9400 Series Supervisor 1 Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis
C9400-SUP-1XL	Cisco Catalyst 9400 Series Supervisor 1XL Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis
C9400-SUP-1XL-Y	Cisco Catalyst 9400 Series Supervisor 25XL Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis

Product ID (append with "=" for spares)	Description
Gigabit Ethernet Switching Modules	
C9400-LC-24S	Cisco Catalyst 9400 Series 24 Port, 1 Gigabit Ethernet SFP module that supports 100/1000 BASET-T with Cu-SFP
C9400-LC-48P	Cisco Catalyst 9400 Series 48 Port, 1 Gigabit Ethernet POE/POE+ module supporting up to 30W per port.
C9400-LC-48S	Cisco Catalyst 9400 Series 48 Port, 1 Gigabit Ethernet SFP module that supports 100/1000 BASET-T with Cu-SFP
C9400-LC-48T	Cisco Catalyst 9400 Series 48-Port 10/100/1000 (RJ-45)
C9400-LC-48U	Cisco Catalyst 9400 Series 48-Port UPOE 10/100/1000 (RJ-45)
Ten Gigabit Ethernet Switching Modules	
C9400-LC-24XS	Cisco Catalyst 9400 Series 24-Port SFP/SFP+ Module
Multigigabit Ethernet Switching Modules	
C9400-LC-48UX	Cisco Catalyst 9400 Series 48-port, UPOE Multigigabit Ethernet Module with: • 24 ports (Ports 1 to 24) 1G UPOE 10/100/1000 (RJ-45) • 24 ports (Ports 25 to 48) MultiGigabit Ethernet 100/1000/2500/5000/10000 UPOE ports
M.2 SATA SSD Modules[1] (for the Supervisor)	
C9400-SSD-240GB	Cisco Catalyst 9400 Series 240GB M2 SATA memory
C9400-SSD-480GB	Cisco Catalyst 9400 Series 480GB M2 SATA memory
C9400-SSD-960GB	Cisco Catalyst 9400 Series 960GB M2 SATA memory
AC Power Supply Modules	
C9400-PWR-2100AC	Cisco Catalyst 9400 Series 2100W AC Power Supply
C9400-PWR-3200AC	Cisco Catalyst 9400 Series 3200W AC Power Supply
DC Power Supply Modules	
C9400-PWR-3200DC	Cisco Catalyst 9400 Series 3200W DC Power Supply

[1] M.2 Serial Advanced Technology Attachment (SATA) Solid State Drive (SSD) Module

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.

Catalyst 9400	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Fuji 16.9.5	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.4	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.3	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.2	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.1	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.8.1a	2.3 Patch 1 2.4	5.4 5.5	PI 3.3 + PI 3.3 latest maintenance release + PI 3.3 latest device pack See Cisco Prime Infrastructure 3.3→ **Downloads**.

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	1024 x 768	Small

[2] We recommend 1 GHz
[3] We recommend 1 GB DRAM

Software Requirements

Operating Systems

- Windows 10 or later

- Mac OS X 10.11 or later

Browsers

- Google Chrome—Version 38 or later (On Windows and Mac)

- Microsoft Edge

- Mozilla Firefox—Version 42 or later (On Windows and Mac)

- Safari—Version 9 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 16.8.1a	CAT9K_IOSXE	cat9k_iosxe.16.08.01a.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.08.01a.SPA.bin

Automatic Boot Loader Upgrade

Automatic Boot Loader Upgrade

Note   If Cisco Catalyst 9400 Series Supervisor 1 Module power is disconnected and reconnected within a 5-second window, the boot SPI may get corrupted.

Caution
- Do not power cycle your switch during an upgrade.

- Do not disconnect power or remove the supervisor module during an upgrade.

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

- Do not perform OIR of a switching module (linecard) when the switch is booting up.

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE Fuji 16.8.1a first time	The boot loader version may be upgraded to 16.6.2r [FC1]. For example:
	
	```ROM: IOS-XE ROMMON```
	```BOOTLDR: System Bootstrap, Version 16.6.2r```
	```[FC1], RELEASE SOFTWARE (P)```
	
	While booting Cisco IOS XE Fuji 16.8.1a, you will see the following on the console:
	
	```%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ###```
	``` BOOTLOADER_UPGRADE skipped```

Complex Programmable Logic Device (CPLD) Upgrade

This refers to hardware-programmable firmware. The CPLD upgrade process is part of the automatic boot loader upgrade. The sequence of events is as follows:

1. The system copies `mcnewfpgaclose.hdr` and `mcnewfpgaclose.img` to the bootflash.

2. The supervisor module then automatically reloads to enable the new boot loader.

3. When the new boot loader boots up, the CPLD upgrade process starts automatically. The CPLD upgrade process takes approximately from 7 to 10 minutes. The supervisor will power cycle itself during the CPLD upgrade.

The following is sample output from a CPLD upgrade:

```
Initializing Hardware...
Initializing Hardware...
Initializing Hardware...

System Bootstrap, Version 16.6.2r, RELEASE SOFTWARE (P)
Compiled Thu 10/26/2017 8:30:34.63 by rel

Current image running:
Primary Rommon Image
Last reset cause: SoftwareResetTrig
C9400-SUP-1 platform with 16777216 Kbytes of main memory

Starting System FPGA Upgrade .....
Programming SPI Primary image is completed.
Authenticating SPI Primary image .....
IO FPGA image is authenticated successfully.

Programming Header .....
FPGA HDR file size: 12
Image page count: 1
Verifying programmed header .....
Verifying programmed header .....
Programmed header is verified successfully.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Power Cycle is needed to complete System firmware upgrade.
It takes ~7 mins to upgrade firmware after power cycle starts.

DO NOT DISRUPT AFTER POWER CYCLE UNTIL ROMMON PROMPT APPEARS.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Power Cycling the Supervisor card now !
Initializing Hardware...
Initializing Hardware...

System Bootstrap, Version 16.6.2r, RELEASE SOFTWARE (P)
Compiled Thu 10/26/2017 8:30:34.63 by rel
Current image running:
Primary Rommon Image
Last reset cause: PowerOn
C9400-SUP-1 platform with 16777216 Kbytes of main memory

rommon 1 >version -v
System Bootstrap, Version 16.6.2r, RELEASE SOFTWARE (P)
Compiled Thu 10/26/2017 8:30:34.63 by rel

Current image running:
Primary Rommon Image
Last reset cause: PowerOn
C9400-SUP-1 platform with 16777216 Kbytes of main memory
Fpga Version: 0x17101705
System Integrity Status: C334ABCE 6A40 6A48
```

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 ...	Permitted Supervisor Setup (Applies to the release you are upgrading from)	First upgrade to...	To upgrade to ...
Cisco IOS XE Everest 16.6.1[4]	Upgrade a single supervisor, and complete the boot loader and CPLD upgrade. After completing the first supervisor upgrade, remove and swap in the second supervisor. After both supervisors are upgraded, they can be inserted and booted in a high availability setup. **Note** Do not simultaneously upgrade dual supervisors from Cisco IOS XE Everest 16.6.1 to a later release. Doing so may cause hardware damage.	Cisco IOS XE Everest 16.6.3 Follow the upgrade steps as in the Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Everest 16.6.x → Upgrading the Switch Software → Upgrading in Install Mode	Cisco IOS XE Fuji 16.8.1a
Cisco IOS XE Everest 16.6.2 and later releases	This procedure automatically copies the images to both active and standby supervisor modules. Both supervisor modules are simultaneously upgraded.	Not applicable	

[4] When upgrading from Cisco IOS XE Everest 16.6.1 to a later release, the upgrade may take a long time, and the system will reset three times due to rommon and complex programmable logic device (CPLD) upgrade. Stateful switchover is supported from Cisco IOS XE Everest 16.6.2

Caution

- Do not power cycle your switch during an upgrade.

- Do not disconnect power or remove the supervisor module during an upgrade.

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

- Do not perform OIR of a switching module (linecard) when the switch is booting up.

The sample output in this section displays upgrade from Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Fuji 16.8.1a using **install** commands.

Procedure

Step 1   Clean Up

a) **install remove inactive**

Use this command to clean up old 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 16 14:14:40 PDT 201
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-cc_srdriver.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.06.01.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:
[R0]:
/flash/cat9k-cc_srdriver.16.06.03.SPA.pkg
/flash/cat9k-espbase.16.06.03.SPA.pkg
/flash/cat9k-rpbase.16.06.03.SPA.pkg
/flash/cat9k-rpboot.16.06.03.SPA.pkg
/flash/cat9k-sipbase.16.06.03.SPA.pkg
/flash/cat9k-sipspa.16.06.03.SPA.pkg
/flash/cat9k-srdriver.16.06.03.SPA.pkg
/flash/cat9k-webui.16.06.03.SPA.pkg
/flash/cat9k_1.bin
/flash/cat9k_1.conf
/flash/cat9k_2.1.conf
/flash/cat9k_2.bin
/flash/cat9k_2.conf
/flash/cat9k_iosxe.16.06.03.SPA.bin
/flash/packages.conf.00-

Do you want to remove the above files? [y/n]y
[R0]:
Deleting file flash:cat9k-cc_srdriver.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.03.SPA.pkg ... done.
Deleting file
Deleting file flash:cat9k-rpbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.03.SPA.pkg ... done.
```

```
Deleting file flash:cat9k-srdriver.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k_1.bin ... done.
Deleting file flash:cat9k_1.conf ... done.
Deleting file flash:cat9k_2.1.conf ... done.
Deleting file flash:cat9k_2.bin ... done.
Deleting file flash:cat9k_2.conf ... done.
Deleting file flash:cat9k_iosxe.16.06.03.SPA.bin ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on Active/Standby
[R0] Post_Remove_Cleanup package(s) on R0
[R0] Finished Post_Remove_Cleanup on R0
Checking status of Post_Remove_Cleanup on [R0]
Post_Remove_Cleanup: Passed on [R0]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Tue Jun 20 14:16:29 PDT 2017
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_iosxe.16.08.01a.SPA.bin flash:

Destination filename [cat9k_iosxe.16.08.01a.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.08.01a.SPA.bin...
Loading /cat9k_iosxe.16.08.01a.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 Mar 16 2018 10:18:11 -07:00 cat9k_iosxe.16.08.01a.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 to flash. 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_iosxe.16.08.01a.SPA.bin activate commit

install_add_activate_commit: START Fri Mar 16 22:49:41 UTC 2018

*Mar 16 22:49:42.772: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 16 22:49:42 install_engine.sh:

 %INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.08.01a.SPA.bin
install_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.08.01a.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

install_add_activate_commit: Activating PACKAGE

/flash/cat9k-webui.16.08.01a.SPA.pkg
/flash/cat9k-srdriver.16.08.01a.SPA.pkg
/flash/cat9k-sipspa.16.08.01a.SPA.pkg
/flash/cat9k-sipbase.16.08.01a.SPA.pkg
/flash/cat9k-rpboot.16.08.01a.SPA.pkg
/flash/cat9k-rpbase.16.08.01a.SPA.pkg
/flash/cat9k-guestshell.16.08.01a.SPA.pkg
/flash/cat9k-espbase.16.08.01a.SPA.pkg
/flash/cat9k-cc_srdriver.16.08.01a.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
[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!

Chassis 1 reloading, reason - Reload command
SUCCESS: install_add_activate_commit
/flash/cat9k-webui.16.08.01a.SPA.pkg
/flash/cat9k-srdriver.16.08.01a.SPA.pkg
/flash/cat9k-sipspa.16.08.01a.SPA.pkg
/flash/cat9k-sipbase.16.08.01a.SPA.pkg
/flash/cat9k-rpboot.16.08.01a.SPA.pkg
/flash/cat9k-rpbase.16.08.01a.SPA.pkg
/flash/cat9k-guestshell.16.08.01a.SPA.pkg
/flash/cat9k-espbase.16.08.01a.SPA.pkg
/flash/cat9k-cc_srdriver.16.08.01a.SPA.pkg
Fri Mar 16 22:53:58 UTC 2018
Switch#
```

Note   Old files listed in the logs will not be removed from flash.

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:/

475140 -rw- 2012104   Jul 26 2017 09:52:41 -07:00 cat9k-cc_srdriver.16.06.03.SPA.pkg
475141 -rw- 70333380  Jul 26 2017 09:52:44 -07:00 cat9k-espbase.16.06.03.SPA.pkg
475142 -rw- 13256     Jul 26 2017 09:52:44 -07:00 cat9k-guestshell.16.06.03.SPA.pkg
475143 -rw- 349635524 Jul 26 2017 09:52:54 -07:00 cat9k-rpbase.16.06.03.SPA.pkg
475149 -rw- 24248187  Jul 26 2017 09:53:02 -07:00 cat9k-rpboot.16.06.03.SPA.pkg
475144 -rw- 25285572  Jul 26 2017 09:52:55 -07:00 cat9k-sipbase.16.06.03.SPA.pkg
475145 -rw- 20947908  Jul 26 2017 09:52:55 -07:00 cat9k-sipspa.16.06.03.SPA.pkg
475146 -rw- 2962372   Jul 26 2017 09:52:56 -07:00 cat9k-srdriver.16.06.03.SPA.pkg
475147 -rw- 13284288  Jul 26 2017 09:52:56 -07:00 cat9k-webui.16.06.03.SPA.pkg
475148 -rw- 13248     Jul 26 2017 09:52:56 -07:00 cat9k-wlc.16.06.03.SPA.pkg

491524 -rw- 25711568  Mar 16 2018 11:49:33 -07:00  cat9k-cc_srdriver.16.08.01a.SPA.pkg
491525 -rw- 78484428  Mar 16 2018 11:49:35 -07:00  cat9k-espbase.16.08.01a.SPA.pkg
491526 -rw- 1598412   Mar 16 2018 11:49:35 -07:00  cat9k-guestshell.16.08.01a.SPA.pkg
491527 -rw- 404153288 Mar 16 2018 11:49:47 -07:00  cat9k-rpbase.16.08.01a.SPA.pkg
491533 -rw- 31657374  Mar 16 2018 11:50:09 -07:00  cat9k-rpboot.16.08.01a.SPA.pkg
491528 -rw- 27681740  Mar 16 2018 11:49:48 -07:00  cat9k-sipbase.16.08.01a.SPA.pkg
491529 -rw- 52224968  Mar 16 2018 11:49:49 -07:00  cat9k-sipspa.16.08.01a.SPA.pkg
491530 -rw- 31130572  Mar 16 2018 11:49:50 -07:00  cat9k-srdriver.16.08.01a.SPA.pkg
491531 -rw- 14783432  Mar 16 2018 11:49:51 -07:00  cat9k-webui.16.08.01a.SPA.pkg
491532 -rw- 9160      Mar 16 2018 11:49:51 -07:00  cat9k-wlc.16.08.01a.SPA.pkg

11353194496 bytes total (9544245248 bytes free)
Switch#
```

   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_iosxe.16.08.01a.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 Mar 16 2018 10:59:16 -07:00 packages.conf
434196 -rw- 7504 Mar 16 2018 10:59:16 -07:00 packages.conf.00-
516098 -rw- 7406 Mar 16 2018 10:58:08 -07:00 cat9k_iosxe.16.08.01a.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

Step 5   Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **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
```

c) **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 16.8.1a image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.08.01a
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.8.1a,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 27-Mar-18 13:43 by mcpre
<output truncated>
```

Downgrading in Install Mode

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

Before you begin

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

When downgrading from ...	Permitted Supervisor Setup (Applies to the release you are downgrading from)	To ...
Cisco IOS XE Fuji 16.8.1a	This procedure automatically copies the images to both active and standby supervisor modules. Both supervisor modules are simultaneously downgraded. **Note** Do not perform an Online Removal and Replacement (OIR) of either supervisor module during the process.	Cisco IOS XE Everest 16.x.x

The sample output in this section shows downgrade from Cisco IOS XE Fuji 16.8.1a to Cisco IOS XE Everest 16.6.2, by using the **install** commands.

Note   New hardware that are introduced in this release cannot be downgraded, so we recommend upgrading all existing switches to Cisco IOS XE Fuji 16.8.1a. For the list of models introduced in this release, see Hardware Features in Cisco IOS XE Fuji 16.8.1a, on page 2

Procedure

Step 1   Clean Up

   a) **install remove inactive**

     Use this command to clean up old 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 16 14:14:40 PDT 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-cc_srdriver.16.08.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.08.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.08.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.08.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.08.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.08.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.08.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.08.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.08.01a.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:
[R0]:
/flash/cat9k-cc_srdriver.16.08.01a.SPA.pkg
/flash/cat9k-espbase.16.08.01a.SPA.pkg
/flash/cat9k-guestshell.16.08.01a.SPA.pkg
/flash/cat9k-rpbase.16.08.01a.SPA.pkg
/flash/cat9k-rpboot.16.08.01a.SPA.pkg
/flash/cat9k-sipbase.16.08.01a.SPA.pkg
/flash/cat9k-sipspa.16.08.01a.SPA.pkg
/flash/cat9k-srdriver.16.08.01a.SPA.pkg
/flash/cat9k-webui.pkg
/flash/cat9k_1.bin
/flash/cat9k_1.conf
/flash/cat9k_2.1.conf
/flash/cat9k_2.bin
/flash/cat9k_2.conf
/flash/cat9k_iosxe.16.08.01a.SSA.bin
/flash/packages.conf.00-

Do you want to remove the above files? [y/n]y
[R0]:
Deleting file flash:cat9k-cc_srdriver.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k_1.bin ... done.
Deleting file flash:cat9k_1.conf ... done.
Deleting file flash:cat9k_2.1.conf ... done.
Deleting file flash:cat9k_2.bin ... done.
Deleting file flash:cat9k_2.conf ... done.
Deleting file flash:cat9k_iosxe.16.08.01a.bin ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on Active/Standby
[R0] Post_Remove_Cleanup package(s) on R0
[R0] Finished Post_Remove_Cleanup on R0
Checking status of Post_Remove_Cleanup on [R0]
Post_Remove_Cleanup: Passed on [R0]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Tue Jun 20 14:16:29 PDT 2017
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_iosxe.16.06.02.SPA.bin flash:

Destination filename [cat9k_iosxe.16.06.02.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.06.02.SPA.bin...
Loading /cat9k_iosxe.16.06.02.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 Mar 16 2018 13:35:16 -07:00 cat9k_iosxe.16.06.02.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3   Downgrade software image

- **install add file activate commit**
- **install rollback to committed**

The following example displays the installation of the cat9k_iosxe.16.06.02.SPA.bin software image to flash, to downgrade the switch 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:
Switch# install add file flash:cat9k_iosxe.16.06.02.SPA.bin activate commit

install_add_activate_commit: START Fri Mar 16 22:49:41 UTC 2018

*Mar 16 22:49:42.772: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 16 22:49:42 install_engine.sh:
%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.06.02.SPA.bininstall_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.06.02.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

install_add_activate_commit: Activating PACKAGE

/flash/cat9k-webui.16.06.02.SPA.pkg
/flash/cat9k-srdriver.16.06.02.SPA.pkg
/flash/cat9k-sipspa.16.06.02.SPA.pkg
/flash/cat9k-sipbase.16.06.02.SPA.pkg
/flash/cat9k-rpboot.16.06.02.SPA.pkg
/flash/cat9k-rpbase.16.06.02.SPA.pkg
/flash/cat9k-espbase.16.06.02.SPA.pkg
/flash/cat9k-cc_srdriver.16.06.02.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
[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!

Chassis 1 reloading, reason - Reload command
SUCCESS: install_add_activate_commit
/flash/cat9k-webui.16.06.02.SPA.pkg
/flash/cat9k-srdriver.16.06.02.SPA.pkg
/flash/cat9k-sipspa.16.06.02.SPA.pkg
/flash/cat9k-sipbase.16.06.02.SPA.pkg
/flash/cat9k-rpboot.16.06.02.SPA.pkg
/flash/cat9k-rpbase.16.06.02.SPA.pkg
/flash/cat9k-guestshell.16.06.02.SPA.pkg
/flash/cat9k-espbase.16.06.02.SPA.pkg
/flash/cat9k-cc_srdriver.16.06.02.SPA.pkg
Fri Mar 16 22:53:58 UTC 2018
Switch#
```

The following example displays sample output when downgrading the switch by using the **install rollback to committed** command.

Important You use the **install rollback to committed** command for downgrading, only if the version you want to downgrade to, is committed.

```
Switch# install rollback to committed
Switch# install rollback to committed

install_rollback: START Thu Nov 2 14:24:56 UTC 2017

This operation requires a reload of the system. Do you want to proceed? [y/n]
*Mar 16 14:24:57.555: %IOSXE-5-PLATFORM: R0/0: Nov 2 14:24:57 install_engine.sh:
%INSTALL-5-INSTALL_START_INFO: Started install rollbacky
--- Starting Rollback ---
Performing Rollback on Active/Standby

WARNING: Found 55 disjoint TDL objects.
[R0] Rollback package(s) on R0
--- Starting rollback impact ---
Changes that are part of this rollback
Current : rp 0 0 rp_boot cat9k-rpboot.16.08.01a.SPA.pkg
Current : rp 1 0 rp_boot cat9k-rpboot.16.08.01a.SPA.pkg
Replacement: rp 0 0 rp_boot cat9k-rpboot.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_boot cat9k-rpboot.16.06.02.SPA.pkg
Current : cc 0 0 cc_srdriver cat9k-cc_srdriver.16.08.01a.SPA.pkg
Current : cc 0 0 cc cat9k-sipbase.16.08.01a.SPA.pkg
Current : cc 0 0 cc_spa cat9k-sipspa.16.08.01a.SPA.pkg
Current : cc 1 0 cc_srdriver cat9k-cc_srdriver.16.08.01a.SPA.pkg
Current : cc 1 0 cc cat9k-sipbase.16.08.01a.SPA.pkg
Current : cc 1 0 cc_spa cat9k-sipspa.16.08.01a.SPA.pkg
Current : cc 10 0 cc cat9k-sipbase.16.08.01a.SPA.pkg
Current : cc 10 0 cc_spa cat9k-sipspa.16.08.01a.SPA.pkg
Current : cc 10 0 cc_srdriver cat9k-cc_srdriver.16.08.01a.SPA.pkg
Current : cc 2 0 cc_srdriver cat9k-cc_srdriver.16.08.01a.SPA.pkg
```

```
Current : cc 2 0 cc cat9k-sipbase.16.08.01a.SPA.pkg
Current : cc 2 0 cc_spa cat9k-sipspa.16.08.01a.SPA.pkg
Current : cc 3 0 cc_srdriver cat9k-cc_srdriver.16.08.01a.SPA.pkg
Current : cc 3 0 cc cat9k-sipbase.16.08.01a.SPA.pkg
Current : cc 3 0 cc_spa cat9k-sipspa.16.08.01a.SPA.pkg
Current : cc 4 0 cc_srdriver cat9k-cc_srdriver.16.08.01a.SPA.pkg
Current : cc 4 0 cc cat9k-sipbase.16.08.01a.SPA.pkg
Current : cc 4 0 cc_spa cat9k-sipspa.16.08.01a.SPA.pkg
Current : cc 5 0 cc_srdriver cat9k-cc_srdriver.16.08.01a.SPA.pkg
Current : cc 5 0 cc cat9k-sipbase.16.08.01a.SPA.pkg
Current : cc 5 0 cc_spa cat9k-sipspa.16.08.01a.SPA.pkg
Current : cc 6 0 cc_srdriver cat9k-cc_srdriver.16.08.01a.SPA.pkg
Current : cc 6 0 cc cat9k-sipbase.16.08.01a.SPA.pkg
Current : cc 6 0 cc_spa cat9k-sipspa.16.08.01a.SPA.pkg
Current : cc 7 0 cc_srdriver cat9k-cc_srdriver.16.08.01a.SPA.pkg
Current : cc 7 0 cc cat9k-sipbase.16.08.01a.SPA.pkg
Current : cc 7 0 cc_spa cat9k-sipspa.16.08.01a.SPA.pkg
Current : cc 8 0 cc_srdriver cat9k-cc_srdriver.16.08.01a.SPA.pkg
Current : cc 8 0 cc cat9k-sipbase.16.08.01a.SPA.pkg
Current : cc 8 0 cc_spa cat9k-sipspa.16.08.01a.SPA.pkg
Current : cc 9 0 cc_srdriver cat9k-cc_srdriver.16.08.01a.SPA.pkg
Current : cc 9 0 cc cat9k-sipbase.16.08.01a.SPA.pkg
Current : cc 9 0 cc_spa cat9k-sipspa.16.08.01a.SPA.pkg
Current : fp 0 0 fp cat9k-espbase.16.08.01a.SPA.pkg
Current : fp 1 0 fp cat9k-espbase.16.08.01a.SPA.pkg
Current : rp 0 0 guestshell cat9k-guestshell.16.08.01a.SPA.pkg
Current : rp 0 0 rp_base cat9k-rpbase.16.08.01a.SPA.pkg
Current : rp 0 0 rp_daemons cat9k-rpbase.16.08.01a.SPA.pkg
Current : rp 0 0 rp_iosd cat9k-rpbase.16.08.01a.SPA.pkg
Current : rp 0 0 rp_security cat9k-rpbase.16.08.01a.SPA.pkg
Current : rp 0 0 rp_webui cat9k-webui.16.08.01a.SPA.pkg
Current : rp 0 0 rp_wlc cat9k-wlc.16.08.01a.SPA.pkg
Current : rp 0 0 srdriver cat9k-srdriver.16.08.01a.SPA.pkg
Current : rp 1 0 guestshell cat9k-guestshell.16.08.01a.SPA.pkg
Current : rp 1 0 rp_base cat9k-rpbase.16.08.01a.SPA.pkg
Current : rp 1 0 rp_daemons cat9k-rpbase.16.08.01a.SPA.pkg
Current : rp 1 0 rp_iosd cat9k-rpbase.16.08.01a.SPA.pkg
Current : rp 1 0 rp_security cat9k-rpbase.16.08.01a.SPA.pkg
Current : rp 1 0 rp_webui cat9k-webui.16.08.01a.SPA.pkg
Current : rp 1 0 rp_wlc cat9k-wlc.16.08.01a.SPA.pkg
Current : rp 1 0 srdriver cat9k-srdriver.16.08.01a.SPA.pkg
Replacement: cc 0 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 0 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 0 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 1 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 1 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 1 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 10 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 10 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 10 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 2 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 2 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 2 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 3 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 3 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 3 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 4 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 4 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 4 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 5 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 5 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 5 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 6 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 6 0 cc cat9k-sipbase.16.06.02.SPA.pkg
```

```
Replacement: cc 6 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 7 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 7 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 7 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 8 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 8 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 8 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 9 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 9 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 9 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: fp 0 0 fp cat9k-espbase.16.06.02.SPA.pkg
Replacement: fp 1 0 fp cat9k-espbase.16.06.02.SPA.pkg
Replacement: rp 0 0 guestshell cat9k-guestshell.16.06.02.SPA.pkg
Replacement: rp 0 0 rp_base cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 0 0 rp_daemons cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 0 0 rp_iosd cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 0 0 rp_security cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 0 0 rp_webui cat9k-webui.16.06.02.SPA.pkg
Replacement: rp 0 0 srdriver cat9k-srdriver.16.06.02.SPA.pkg
Replacement: rp 1 0 guestshell cat9k-guestshell.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_base cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_daemons cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_iosd cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_security cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_webui cat9k-webui.16.06.02.SPA.pkg
Replacement: rp 1 0 srdriver cat9k-srdriver.16.06.02.SPA.pkg
Finished rollback impact
[R0] Finished Rollback on R0
Checking status of Rollback on [R0]
Rollback: Passed on [R0]
Finished Rollback

Install will reload the system now!
SUCCESS: install_rollback Thu Nov 2 14:26:35 UTC 2017

Switch#
*Mar 16 14:26:35.880: %IOSXE-5-PLATFORM: R0/0: Mar 16 14:26:35 install_engine.sh:
%INSTALL-5-INSTALL_COMPLETED_INFO: Completed install rollback PACKAGE
*Mar 16 14:26:37.740: %IOSXE_OIR-6-REMCARD: Card (rp) removed from slot R1
*Mar 16 14:26:39.253: %IOSXE_OIR-6-INSCARD: Card (rp) inserted in slot R1Nov 2 14:26:5

Initializing Hardware...

System Bootstrap, Version 16.8.1r[FC1], RELEASE SOFTWARE (P)
Compiled Tue 10/31/2017 11:38:44.98 by rel

Current image running:
Primary Rommon Image

Last reset cause: SoftwareResetTrig
C9400-SUP-1 platform with 16777216 Kbytes of main memory

Preparing to autoboot. [Press Ctrl-C to interrupt] 0
attempting to boot from [bootflash:packages.conf]

Located file packages.conf
#
###############################################################################################################################################################################################################


Warning: ignoring ROMMON var "BOOT_PARAM"
Warning: ignoring ROMMON var "USER_BOOT_PARAM"

Restricted Rights Legend
```

```
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706




Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.2,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Sat 22-Jul-17 05:51 by mcpre




Cisco IOS-XE software, Copyright (c) 2005-2017 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.




FIPS: Flash Key Check : Begin
FIPS: Flash Key Check : End, Not Found, FIPS Mode Not Enabled

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco C9410R (X86) processor (revision V00) with 868521K/6147K bytes of memory.
Processor board ID FXS2118Q1GM
312 Gigabit Ethernet interfaces
40 Ten Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
15958516K bytes of physical memory.
11161600K bytes of Bootflash at bootflash:.
1638400K bytes of Crash Files at crashinfo:.
0K bytes of WebUI ODM Files at webui:.
```

```
%INIT: waited 0 seconds for NVRAM to be available

Press RETURN to get started!
```

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 Everest 16.6.2 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.06.02
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Fri 16-Mar-18 06:38 by mcpre
<output truncated>
```

Licensing

This section provides information about the licensing packages for features available on Cisco Catalyst 9000 Series Switches.

License Levels

The software features available on Cisco Catalyst 9400 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://www.cisco.com/go/cfn. 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.

Using Smart Accounts

We recommend that you assign a Smart Account when you order devices or licenses. Smart Accounts enable you to manage all of your software licenses for switches, routers, firewalls, access-points or tools from one centralized website.

- Create Smart Accounts by going to https://software.cisco.com → **Administration** → **Request Smart Account**.

- Manage your licenses by going to https://software.cisco.com → **Administration** → **Manage Smart Account**.

Note This is especially relevant to the term licenses that you order, because information about the expiry of term licenses is available only through your Smart Account.

For more information about Smart Accounts and Smart Software Licensing in general, go to the Cisco Smart Software Manager (Cisco SSM) website on cisco.com: http://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html

The possible deployment modes are:

- The right-to-use (RTU) licensing mode—Supported on Cisco Catalyst 9000 Series Switches. See The RTU Licensing Mode.

- The Smart Licensing mode—Currently not supported on Cisco Catalyst 9000 Series Switches. It is on the roadmap for future releases.

The RTU Licensing Mode

This is the currently supported licensing mode for Cisco Catalyst 9000 Series Switches.

Right-to-use (RTU) licensing allows you to order and activate a specific license type for a given license level, and then to manage license usage on your switch.

Note   The RTU licensing structure has been modified to match the packaging model that will be used with Smart Licensing mode in the future. Unified licensing structures across the RTU and Smart Licensing modes, along with usage reports, will simplify migration and reduce the implementation time required for Smart Licensing.

The **license right-to-use** command (privilege EXEC mode) provides options to activate or deactivate any license supported on the platform.

Options for Base Licenses

```
license right-to-use[{activate|deactivate}][{network-essentials|
network-advantage}][{all|evaluation|subscription}][{active|both|
standby}][{acceptEULA}]
```

Options for Add-On Licenses

```
license right-to-use[{activate|deactivate}]addon{dna-essentials|
dna-advantage}{evaluation|subscription}[{active|both|standby}][{acceptEULA}]
```

Usage Guidelines for the RTU Licensing Mode

- Base licenses (Network Essentials and Network-Advantage) may be ordered only with a permanent license type.

- Add-on licenses (DNA Essentials and DNA Advantage) may be ordered only with a term license type.

- You can set up Cisco SSM to receive daily e-mail alerts, to be notified of expiring add-on licenses that you want to renew.

- You must order an add-on license in order to purchase a switch. On term expiry, you can either renew the add-on license to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.

- When ordering an add-on license with a base license, note the combinations that are permitted and those that are not permitted:

Table 1: Permitted Combinations

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

[5] For this combination, the DNA-Essentials license must be ordered separately using Cisco SSM.

- The following features are currently available only at the Network Advantage license level. However, the correct minimum license level for these features is Network Essentials and the CFN reflects this correct license level. You will be able to configure these features with a Network Essentials license level after the correction is made in an upcoming release:

    - IPv6 Multicast

    - IPv6 ACL Support for HTTP Servers

- Evaluation licenses cannot be ordered. They can be activated temporarily, without purchase. Warning system messages about the evaluation license expiry are generated 10 and 5 days before the 90-day window. Warning system messages are generated every day after the 90-day period. An expired evaluation license cannot be reactivated after reload.

For detailed configuration information about using the RTU Licensing Mode, see the *System Management Configuration Guide → Configuring Right-To-Use Licenses* chapter for your release.

Scaling Guidelines

For information about feature scaling guidelines, see these datasheets for Cisco Catalyst 9400 Series Switches:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9600-series-line-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-sup-eng-data-sheet-cte-en.html

Limitations and Restrictions

- Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.

- 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.

- Flexible NetFlow limitations

    - You cannot configure NetFlow export using the Ethernet Management port (GigabitEthernet0/0).

    - You can not configure a flow monitor on logical interfaces, such as switched virtual interfaces (SVIs), port-channel, loopback, tunnels.

    - You can not configure multiple flow monitors of same type (ipv4, ipv6 or datalink) on the same interface for same direction.

- Hardware limitations: When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, autonegotiation is enabled by default. If the other end of the line does not support autonegotation, the link does not come up.

- Interoperability limitations:

    - When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, if one end of the 40G link is a Catalyst 9400 Series Switch and the other end is a Catalyst 9500 Series Switch, the link

does not come up, or comes up on one side and stays down on the other. To avoid this interoperability issue between devices, apply the the **speed nonegotiate** command on the Catalyst 9500 Series Switch interface. This command disables autonegotiation and brings the link up. To restore autonegotiation, use the **no speed nonegotiation** command.

- Memory leak—When a logging discriminator is configured and applied to a device, memory leak is seen under heavy syslog or debug output. The rate of the leak is dependent on the quantity of logs produced. In extreme cases, the device may fail. As a workaround, disable the logging discriminator on the device.

- No service password recovery—With ROMMON versions R16.6.1r and R16.6.2r, the 'no service password-recovery' feature is not available.

- 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.

- Redundancy—The supervisor module (hardware) supports redundancy. Software redundancy is supported starting with Cisco IOS XE Everest 16.6.2. However, the associated route processor redundancy (RPR) feature is not supported.

    Before performing a switchover, use the **show redundancy**, **show platform**, and **show platform software iomd redundancy** commands to ensure that both the SSOs have formed and that the IOMD process is completed.

    In the following sample output for the **show redundancy**, note that both the SSOs have formed.

```
Switch# show redundancy
Redundant System Information :
------------------------------
Available system uptime = 3 hours, 30 minutes
Switchovers system experienced = 2
Standby failures = 0
Last switchover reason = active unit removed

Hardware Mode = Duplex
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Maintenance Mode = Disabled
Communications = Up

Current Processor Information :
-------------------------------
Active Location = slot 3
Current Software state = ACTIVE
Uptime in current state = 2 hours, 57 minutes
Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE),
Version 16.8.1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 27-Mar-18 13:43 by mcpre
BOOT = bootflash:packages.conf;
CONFIG_FILE =
Configuration register = 0x1822

Peer Processor Information :
----------------------------
```

```
Standby Location = slot 4
Current Software state = STANDBY HOT
Uptime in current state = 2 hours, 47 minutes
Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE),
Version 16.8.1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 27-Mar-18 13:43 by mcpre
BOOT = bootflash:packages.conf;
CONFIG_FILE =
Configuration register = 0x1822
```

In the following sample output for the **show platform** command, note that both SSOs have formed and the HA_STATE field is ready.

```
Switch# show platform
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Local RF state = ACTIVE
Peer RF state = STANDBY HOT

slot  PSM STATE   SPA INTF   HA_STATE HA_ACTIVE
   1    ready    started    ready    00:01:16
   2    ready    started    ready    00:01:22
   3    ready    started    ready    00:01:27 ***active RP
   4    ready    started    ready    00:01:27
<output truncated>
```

In the following sample output for the **show platform software iomd redundancy** command, note that the state for all the linecards and supervisor modules is ok. This indicates that the IOMD processes are completed.

```
Switch# show platform software iomd redundancy
Chassis type: C9407R

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
1         C9400-LC-24XS       ok                    3d09h
2         C9400-LC-48U        ok                    3d09h
R0        C9400-SUP-1         ok, active            3d09h
R1        C9400-SUP-1         ok, standby           3d09h
P1        C9400-PWR-3200AC    ok                    3d08h
P2        C9400-PWR-3200AC    ok                    3d08h
P17       C9407-FAN           ok                    3d08h
<output truncated>
```

- With bootloader version 16.6.2r, you cannot access the M.2 SATA SSD drive at the ROMMON prompt (rommon> **dir disk0**). The system displays an error message indicating that the corresponding file system protocol is not found on the device. The only way to access the drive when on bootloader version 16.6.2r, is through the Cisco IOS prompt, after boot up.

- 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.

- Uplink Symmetry—When a redundant supervisor module is inserted, we recommend that you have symmetric uplinks, to minimize packet loss during a switchover.

  Uplinks are said to be in symmetry when the same interface on both supervisor modules have the same type of transceiver module. For example, a TenGigabitEthernet interface with no transceiver installed operates at a default 10G mode; if the matching interface of the other supervisor has a 10G transceiver, then they are in symmetry. Symmetry provides the best SWO packet loss and user experience.

  Asymmetric uplinks have at least one or more pairs of interfaces in one supervisor not matching the transceiver speed of the other supervisor.

- 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.

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 16.8.x

Caveat ID Number	Description
CSCvg53159	%SNMP-3-RESPONSE_DELAYED: processing GetNext of cafSessionEntry.2 seen on catalyst switch
CSCvh52491	AVB : FED_QOS_ERRMSG-3-QUEUE_BUFFER_HW_ERROR on shutting down neigh port connected to msrp listener
CSCvh63530	MPLS traffic drops with ECMP loadbalance towards core. All cat9ks
CSCvh74803	C9400: Chassis SYSTEM_SERIAL_NUMBER not available for iPXE boot
CSCvh97897	Copper GE T SFP not able detect by system SW after optic OIR
CSCvi27622	Switch fails to recognize SUP when OIR is repeated in a certain sequence
CSCvi70461	C9400 - Power Redundancy n+n not keeping stdby power supplies in active mode after user intervention

Caveat ID Number	Description
CSCvg86020	Cat9400: after SWO, traffic drop is seen on uplinks for longer duration only if speeds is 100m
CSCvh24952	C9400: Need to remove AP count keyword from license options.
CSCvh72186	Cat9k ROMMON: HTTP booting does not allow specified port number
CSCvh74803	C9400: Chassis SYSTEM_SERIAL_NUMBER not available for iPXE boot
CSCvh79433	C9400: "kernel: ICMPv6: NA: someone advertises our address" seen when neighbor bootup
CSCvh63530	MPLS traffic drops with ECMP loadbalance towards core. All cat9ks
CSCvh80159	C9400: %BOOT-3-SYSD_STARTFAIL: R0/0: Failed to launch boot task binos_script.service (exit-code)
CSCvh84345	IOS CLI "show platform software fed switch active punt cause summary" may display negative counts
CSCvi13167	16.8.1: Traffic drops to 50% after SW when there is mulitple core facing SVI
CSCvi33452	C9400 Got Traceback while doing VLAN shut/noshut after SSO
CSCvi50604	C9400: After switchover Webauth is not working in 16.8.1 PRD6 FC1
CSCvi69699	9400 - 9300: 40G copper QSFP interoperability broken (link down) after CSCvh28104 commit in 16.8.1
CSCvi71691	On sup removal, all ports on LC C9400-LC-48UX drop about 3 to 4 percent traffic
CSCvi75488	Ping from client fails with enforcement enabled on known mappings
CSCvi78178	SUP-1 and SUP-1XL should not form HA
CSCvi81086	In N+N redundancy mode, running different capacity pwr supply, "Full protected" state not guaranteed

Resolved Caveats in Cisco IOS XE Fuji 16.8.1a

Caveat ID Number	Description
CSCve21940	C9400 Cannot ping phone/data client with IPSG
CSCvf20603	entities for a power supply may not be grouped together in entity-mib after oir into different slots
CSCvg13725	C9400: No syslog generated when toggling the fan tray beacon manually
CSCvg26395	40G Traffic loss due to NRU transit path latency
CSCvg56874	9400: System LED became RED after Active SUP OIR

Caveat ID Number	Description
CSCvh50172	MPLS L3VPN traffic is dropped due to Wrong bgp vpn label (exp null)
CSCvh66534	16.8.1 pwr-state toggling during LC boot up cause cmcc crash
CSCvh71930	show chassis power-supply detail report "PEC error"
CSCvi19809	Memory leak on C9300 due TMS process
CSCvi69699	9400 - 9300: 40G copper QSFP interoperability broken (link down)

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 16 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 9400 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9400-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: http://www.cisco.com/go/mibs

Communications, Services, and Additional Information

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

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.