Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Amsterdam 17.1.x

First Published: 2019-11-26

Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Amsterdam 17.1.x

Introduction

Cisco Catalyst 9400 Series Switches are Cisco's leading modular enterprise switching access platform and have 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 Unified Access Data Plane (UADP) 2.0 and UADP 3.0. 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). This 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

Whats New in Cisco IOS XE Amsterdam 17.1.1

Hardware Features in Cisco IOS XE Amsterdam 17.1.1

There are no new hardware features in this release

Software Features in Cisco IOS XE Amsterdam 17.1.1

Feature Name	Description, Documentation Link, and License Level Information
BIOS Protection for Golden SPI	Enables write-protection of the golden ROMMON image. See System Management → BIOS Protection. (Network Essentials and Network Advanatge)

Feature Name	Description, Documentation Link, and License Level Information
ERSPAN IPv6	Introduces IPv6 support for Encapsulated Remote Switched Port Analyzer (ERSPAN). ERSPAN enables you to monitor traffic on ports or VLANs, and send the monitored traffic to destination ports. See Network Management → Configuring ERSPAN. (DNA Advantage)
Flash MIB instance retrieval count limit increase	The limitation of Flash MIB listing 100 files per partition per device has been removed. Flash MIB can now fetch all the files from the flash file system. See Network Management → Configuring Simple Network Management Protocol. (Network Essentials and Network Advantage)
IGMP (IPv4) : VPLS Layer 2 Snooping	Introduces support for Internet Group Management Protocol (IGMP) snooping on a Virtual Private LAN Service (VPLS) configured network. See Multiprotocol Label Switching → Configuring Virtual Private LAN Service (VPLS) and VPLS BGP-Based Autodiscovery. (Network Advantage)
Ingress and Egress Flexible Netflow on MPLS	Allows capture of IP flow information for packets undergoing Multiprotocol Label Switching (MPLS) label imposition when entering an MPLS network. These packets arrive on a device as IP packets and are transmitted as MPLS packets. Enable the feature by configuring an ingress flow monitor for IPv4 and IPv6 traffic at the customer edge (CE) facing side of the provider edge (PE) node. See Network Management → Configuring Flexible NetFlow. (DNA Essentials and DNA Advantage)
MACsec over Ethernet over MPLS (EoMPLS)	In VLAN mode, the switch (PE device) can now process packets in which the 802.1Q tag is not encrypted by the CE device. See Multiprotocol Label Switching → Configuring Ethernet-over-MPLS (EoMPLS). (Network Advantage)
MPLS VPN InterAS Option A	MPLS VPN InterAS options provide multiple ways of interconnecting VPNs between different MPLS VPN service providers. With one of the options configured, a customer's site can exist on several carrier networks (autonomous systems) and still have seamless VPN connectivity. Of the available InterAS options, MPLS VPN InterAS Option A is the simplest to configure. This option provides back-to-back virtual routing and forwarding (VRF) connectivity (MPLS VPN providers exchange routes across VRF interfaces). See Multiprotocol Label Switching → Configuring MPLS VPN InterAS Options. (Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Multicast VPN Extranet Support	Enables service providers to distribute IP multicast content originating from one enterprise site to other enterprise sites. See IP Multicast Routing → Configuring Multicast VPN Extranet Support. (Network Advantage)
Neighbor Discovery (ND) Inspection Feature Deprecation	The IPv6 ND Inspection feature is deprecated. The Switch Integrated Security Features based (SISF-based) device tracking feature replaces it and offers the same capabilities. See Security → Configuring IPv6 First Hop Security. (Network Essentials and Network Advantage)
Network Address Translation (NAT)	Enables private IP networks that use unregistered IP addresses, to connect to the Internet. NAT operates on a device, usually connecting two networks together, and translates the private addresses in the internal network into global routable addresses, before packets are forwarded onto another network. See IP Addressing Services → Configuring Network Address Translation. (Network Advantage)
Opening or Closing SNMP UDP Ports	A security enhancement that enables you to access the Simple Network Management Protocol (SNMP) UDP ports only after one of the requisite commands is configured. This design change secures and opens the ports only when required and prevents a device from listening to a port unnecessarily. See Network Management → Configuring Simple Network Management Protocol. (Network Essentials and Network Advantage)
Per-Port MTU Configuration	Introduces support for port level and port channel level maximum transmission unit (MTU) configuration. With Per-Port MTU configuration, you can configure different MTU values for different interfaces as well as for different port channel interfaces. See Interface and Hardware Components → Configuring Per-Port MTU. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Programmability • Application Hosting • Candidate Configuration Commit Confirm • Model-Driven Telemetry Event Notification Support • RESTCONF YANG-Patch Support • Python 3 Support in Guest Shell • TLS for gRPC Dial-Out • SGACL and Environment Data Download over REST	The following programmability features are introduced in this release: • Application Hosting: Introduces support for application hosting on the management interface and front-panel ports. Cisco Catalyst 9400 Series Switches use the M2 SATA module for application hosting; applications can be hosted on C9400-SSD-240GB, C9400-SSD-480GB, and C9400-SSD-960GB solid state drives (SSDs). **Note** The Cisco Catalyst 9410R switch does not support front-panel application-hosting. • The candidate configuration supports the confirmed commit capability. This implementation is as specified in RFC 6241 for the confirmed commit capability which, when issued, sets the running configuration to the current contents of the candidate configuration and starts a confirmed commit timer. The confirmed commit operation will be rolled back if the commit is not issued within the timeout period. The default timeout period is 600 seconds or 10 minutes. • Model-Driven Telemetry Event Notification Support: Introduces support for event notifications over the NETCONF protocol. • RESTCONF YANG-Patch Support: Introduces support for YANG-Patch media type as specified by RFC 8072. • Python 3 Support in Guest Shell: Introduces support for Python Version 3.6 is supported in Guest Shell. • TLS for gRPC Dial-Out: Introduces support for TLS for gRPC dial-out. • Cisco TrustSec uses the REST-based transport protocol for SGACL policy provisioning and data download from Cisco Identity Services Engine (ISE). The REST-based protocol is more secure, and provides reliable, and faster policy and environment data provisioning, than the RADIUS protocol that is used in previous releases. Both the REST API-based and RADIUS-based download of Cisco TrustSec data is supported. However, only one protocol can be active on a device. In Cisco IOS XE Amsterdam 17.1.1, REST-based protocol is the default. • 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/1711. Some of the models introduced in this release are not backward compatible. For the complete list, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1711/BIC. Revision statements embedded in the YANG files indicate if there has been a model revision. The *README.md* file in the same GitHub location highlights changes that have been made in the release. See Programmability. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
VPLS Flow-Aware Transport Pseudowire Support	Provides the capability to identify individual flows within a pseudowire and provides devices the ability to use these flows to load-balance traffic. See Multiprotocol Label Switching → Configuring Virtual Private LAN Service (VPLS) and VPLS BGP-Based Autodiscovery. (Network Advantage)
VPLS Protocol-Mode CLI Support	Introduces support for VPLS and VPLS BGP-based Autodiscovery configurations using protocol-CLI mode. See Multiprotocol Label Switching → Configuring Virtual Private LAN Service (VPLS) and VPLS BGP-Based Autodiscovery. (Network Advantage)

New on the Web UI	
• New default credentials for WebUI • Power Over Ethernet (POE) • Intermediate System-Intermediate System(IS-IS) • Routing Information Protocol (RIP) • Virtual Terminal Lines (VTY)	Use the WebUI for: • New default credentials for WebUI—The login credentials for connecting to the device from the WebUI at Day 0 have been updated. This is available in the respective platform hardware guide. • Power Over Ethernet (POE)—The dashboard displays a dashlet for POE utilization for the switch. • Intermediate System- Intermediate System(IS-IS)—Supports Integrated Intermediate System-Intermediate System(IS-IS) routing protocol configuration for improved routing of data packets to their destination based on the best route. • Routing Information Protocol (RIP)—Supports RIP configuration for improved routing of data packets to their destination based on the hop count. • Virtual Terminal Lines (VTY)—Supports vty lines configuration in device setup, to allow a maximum number of simultaneous access to the device, remotely, through Telnet or SSH.

Important Notes

• Cisco StackWise Virtual - Supported and Unsupported Features, on page 5
• Unsupported Features, on page 6
• Complete List of Supported Features, on page 6
• Accessing Hidden Commands, on page 6
• Default Behaviour, on page 7

Cisco StackWise Virtual - Supported and Unsupported Features

When you enable Cisco StackWise Virtual on the device

- Layer 2, Layer 3, Security, Quality of Service, Multicast, Application, Monitoring and Management, Multiprotocol Label Switching, High Availability, and VXLAN BGP EVPN are supported.

  Contact the Cisco Technical Support Centre for the specific list of features that are supported under each one of these technologies.

- Resilient Ethernet Protocol, Remote Switched Port Analyzer, and Sofware-Defined Access are NOT supported

Unsupported Features

- Audio Video Bridging (including IEEE802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav)
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Converged Access for Branch Deployments
- Fast PoE
- IPsec VPN
- MACsec Switch to Switch Connections on C9400-SUP-1XL-Y.
- 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 not equipped with CLI help. This means that entering a question mark (?) at the system prompt does not display the list of available commands. These commands are only meant to assist Cisco TAC in advanced troubleshooting and are not documented either.

Hidden commands are available under:

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

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

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

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

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

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

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

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

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

Default Behaviour

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

Supported Hardware

Cisco Catalyst 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

Switch Model (append with "=" for spares)	Description
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.
Line Cards	
C9400-LC-24S	24-port, 1 Gigabit Ethernet SFP module that supports 100/1000 BASET-T with Cu-SFP
C9400-LC-24XS	24-port Gigabit Ethernet module that supports 1 and 10 Gbps connectivity.
C9400-LC-48H	48-port Gigabit Ethernet UPOE+ module supporting up to 90W on each of its 48 RJ45 ports.
C9400-LC-48P	48-port, 1 Gigabit Ethernet POE/POE+ module supporting up to 30W per port.
C9400-LC-48S	48-port, 1 Gigabit Ethernet SFP module that supports 100/1000 BASET-T with Cu-SFP.
C9400-LC-48T	48-port, 10/100/1000 BASE-T Gigabit Ethernet module.

Product ID (append with "=" for spares)	Description
C9400-LC-48U	48-port UPOE 10/100/1000 (RJ-45) module supporting up to 60W per port.
C9400-LC-48UX	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

To view the software compatibility information between Cisco Catalyst 9400 Series Switches, Cisco Identity Services Engine, and Cisco Prime Infrastructure, go to Cisco Catalyst 9000 Series Switches Software Version Compatibility Matrix.

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)

ROMMON and CPLD Versions

This topic list the ROMMON and CPLD versions for Cisco Catalyst 9400 Series Switches.

ROMMON

ROMMON, also known as the boot loader, is firmware that runs when the device is powered up or reset. It initializes the processor hardware and boots the operating system software (Cisco IOS XE software image). The ROMMON is stored on the following Serial Peripheral Interface (SPI) flash devices on your switch:

- Primary: The ROMMON stored here is the one the system boots every time the device is powered-on or reset.
- Golden: The ROMMON stored here is a backup copy. If the one in the primary is corrupted, the system automatically boots the ROMMON in the golden SPI flash device.

ROMMON upgrades may be required to resolve firmware defects, or to support new features, but there may not be new versions with every release. A Cisco IOS XE release is also compatible with a ROMMON version lower or higher than what is specified in this table. For more information, see "Upgrading the ROMMON" section.

Complex Programmable Logic Device (CPLD)

CPLD refers to hardware-programmable firmware. We recommend that you perform CPLD upgrade to resolve firmware defects or to support new features. There may not be new CPLD versions with every release.

If your device is running CPLD version 0x171017, you must upgrade to a later version. Every IOS XE version has a specific CPLD version bundled with it as shown in the table below. If your device is running CPLD version lower than the version bundled with the IOS XE image, we recommend you upgrade the CPLD. IOS XE does not allow CPLD downgrade. For information on how to perform CPLD upgrade, refer Upgrading the Complex Programmable Logic Device Version, on page 27.

This table provides ROMMON and CPLD version information for the Cisco Catalyst 9400 Series Supervisor Modules. For ROMMON and CPLD version information of Cisco IOS XE 16.x.x releases, refer to the corresponding Cisco IOS XE 16.x.x release notes of the respective platform.

Release	ROMMON Version (C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y)	CPLD Version (C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y)	ROMMON Version (C9400X-SUP-2, C9400X-SUP-2XL)	CPLD Version (C9400X-SUP-2, C9400X-SUP-2XL)
Amsterdam 17.1.1	17.1.1r	19032905	-	-

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 Amsterdam 17.1.1	CAT9K_IOSXE	cat9k_iosxe.17.01.01.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.01.01.

Upgrading the ROMMON

To know the ROMMON or bootloader version that applies to every major and maintenance release, see ROMMON and CPLD Versions, on page 10.

You can upgrade the ROMMON before, or, after upgrading the software version. If a new ROMMON version is available for the software version you are upgrading to, proceed as follows:

- Upgrading the ROMMON in the primary SPI flash device

  This ROMMON is upgraded automatically. When you upgrade from an existing release on your switch to a later or newer release for the first time, and there is a new ROMMON version in the new release, the system automatically upgrades the ROMMON in the primary SPI flash device, based on the hardware version of the switch when you boot up your switch with the new image for the first time.

- Upgrading the ROMMON in the golden SPI flash device

  You must manually upgrade this ROMMON. Enter the **upgrade rom-monitor capsule golden switch** command in privileged EXEC mode.



Note In case of a Cisco StackWise Virtual setup, upgrade the active and standby switch.

In case of a High Availability set up, upgrade the active and standby switch.

After the ROMMON is upgraded, it will take effect on the next reload. If you go back to an older release after this, the ROMMON is not downgraded. The updated ROMMON supports all previous releases.

Software Installation Commands

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

Upgrading in Install Mode

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

Before you begin

Caution You must comply with these cautionary guidelines during an upgrade:

- Do not power cycle the switch.
- Do not disconnect power or remove the supervisor module.
- 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 an OIR of a switching module (linecard) when the switch is booting up.

Note Disconnecting and reconnecting power to a Cisco Catalyst 9400 Series Supervisor 1 Module within a 5-second window, can corrupt the boot SPI.

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 Amsterdam 17.1.1
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 Gibraltar 16.12.1 to Cisco IOS XE Amsterdam 17.1.1 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 Wed Nov 20 14:14:40 PDT 2019
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.12.01.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.16.12.01.SPA.pkg
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
/flash/cat9k-webui.16.12.01.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.17.01.01.SPA.bin

/flash/packages.conf.00-

Do you want to remove the above files? [y/n]y
[R0]:
Deleting file flash:cat9k-cc_srdriver.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.17.01.01.SPA.pkg ... done.
Deleting file
Deleting file flash:cat9k-rpbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.17.01.01.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 Wed Nov 20 14:16:29 PDT 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6// flash:

Destination filename [cat9k_iosxe.17.01.01.SPA.bin
]?
Accessing tftp://10.8.0.6//cat9k_iosxe.17.01.01.SPA.bin
...
Loading /cat9k_iosxe.17.01.01.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 Nov 20 2019 10:18:11 -07:00 cat9k_iosxe.17.01.01.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 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.17.01.01.SPA.bin
 activate commit

install_add_activate_commit: START Wed Nov 20 22:49:41 UTC 2019

*Nov 20 22:49:42.772: %IOSXE-5-PLATFORM: Switch 1 R0/0: Nov 20 22:49:42 install_engine.sh:

 %INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.17.01.01.SPA.bin

install_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.17.01.01.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

install_add_activate_commit: Activating PACKAGE

/flash/cat9k-webui.17.01.01.SPA.pkg
/flash/cat9k-srdriver.17.01.01.SPA.pkg
/flash/cat9k-sipspa.17.01.01.SPA.pkg
/flash/cat9k-sipbase.17.01.01.SPA.pkg
/flash/cat9k-rpboot.17.01.01.SPA.pkg
/flash/cat9k-rpbase.17.01.01.SPA.pkg
/flash/cat9k-guestshell.17.01.01.SPA.pkg
/flash/cat9k-espbase.17.01.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.01.01.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
[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.17.01.01.SPA.pkg
/flash/cat9k-srdriver.17.01.01.SPA.pkg
/flash/cat9k-sipspa.17.01.01.SPA.pkg
/flash/cat9k-sipbase.17.01.01.SPA.pkg
/flash/cat9k-rpboot.17.01.01.SPA.pkg
/flash/cat9k-rpbase.17.01.01.SPA.pkg
/flash/cat9k-guestshell.17.01.01.SPA.pkg
/flash/cat9k-espbase.17.01.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.01.01.SPA.pkg
Wed Nov 20 22:53:58 UTC 2019
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 ten new `.pkg` files and two `.conf` files.

```
Switch# dir flash:

Directory of flash:/
475140 -rw- 2012104   Jul 31 2019 09:52:41 -07:00 cat9k-cc_srdriver.16.12.01.SPA.pkg
475141 -rw- 70333380  Jul 31 2019 09:52:44 -07:00 cat9k-espbase.16.12.01.SPA.pkg
475142 -rw- 13256     Jul 31 2019 09:52:44 -07:00 cat9k-guestshell.16.12.01.SPA.pkg
475143 -rw- 349635524 Jul 31 2019 09:52:54 -07:00 cat9k-rpbase.16.12.01.SPA.pkg
475149 -rw- 24248187  Jul 31 2019 09:53:02 -07:00 cat9k-rpboot.16.12.01.SPA.pkg
475144 -rw- 25285572  Jul 31 2019 09:52:55 -07:00 cat9k-sipbase.16.12.01.SPA.pkg
475145 -rw- 20947908  Jul 31 2019 09:52:55 -07:00 cat9k-sipspa.16.12.01.SPA.pkg
475146 -rw- 2962372   Jul 31 2019 09:52:56 -07:00 cat9k-srdriver.16.12.01.SPA.pkg
475147 -rw- 13284288  Jul 31 2019 09:52:56 -07:00 cat9k-webui.16.12.01.SPA.pkg
475148 -rw- 13248     Jul 31 2019 09:52:56 -07:00 cat9k-wlc.16.12.01.SPA.pkg

491524 -rw- 25711568  Nov 20 2019 11:49:33 -07:00  cat9k-cc_srdriver.17.01.01.SPA.pkg
491525 -rw- 78484428  Nov 20 2019 11:49:35 -07:00  cat9k-espbase.17.01.01.SPA.pkg
491526 -rw- 1598412   Nov 20 2019 11:49:35 -07:00  cat9k-guestshell.17.01.01.SPA.pkg
491527 -rw- 404153288 Nov 20 2019 11:49:47 -07:00  cat9k-rpbase.17.01.01.SPA.pkg
491533 -rw- 31657374  Nov 20 2019 11:50:09 -07:00  cat9k-rpboot.17.01.01.SPA.pkg
491528 -rw- 27681740  Nov 20 2019 11:49:48 -07:00  cat9k-sipbase.17.01.01.SPA.pkg
491529 -rw- 52224968  Nov 20 2019 11:49:49 -07:00  cat9k-sipspa.17.01.01.SPA.pkg
491530 -rw- 31130572  Nov 20 2019 11:49:50 -07:00  cat9k-srdriver.17.01.01.SPA.pkg
491531 -rw- 14783432  Nov 20 2019 11:49:51 -07:00  cat9k-webui.17.01.01.SPA.pkg
491532 -rw- 9160      Nov 20 2019 11:49:51 -07:00  cat9k-wlc.17.01.01.SPA.pkg

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

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

- `packages.conf`—the file that has been re-written with the newly installed .pkg files
- `cat9k_iosxe.17.01.01.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 Nov 20 2018 10:59:16 -07:00 packages.conf
516098 -rw- 7406 Nov 20 2018 10:58:08 -07:00 cat9k_iosxe.17.01.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

Step 5 Verify installation

show version

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

The following sample output of the **show version** command displays the Cisco IOS XE Amsterdam 17.1.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.01.01
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.1.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
<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 Amsterdam 17.1.1	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 Gibraltar 16.12.x or earlier releases.

The sample output in this section shows downgrade from Cisco IOS XE Amsterdam 17.1.1 to Cisco IOS XE Gibraltar 16.12.1c, using **install** commands.

Important New hardware modules (supervisors or line card modules) 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 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 Wed 20 Nov 14:14:40 PDT 2019
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.17.01.01.SPA.pkg
File is in use, will not delete.
cat9k-espbase.17.01.01.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.17.01.01.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.17.01.01.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.17.01.01.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.17.01.01.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.17.01.01.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.17.01.01.SPA.pkg
File is in use, will not delete.
cat9k-webui.17.01.01.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.17.01.01.SPA.pkg
/flash/cat9k-espbase.17.01.01.SPA.pkg
/flash/cat9k-guestshell.17.01.01.SPA.pkg
/flash/cat9k-rpbase.17.01.01.SPA.pkg
/flash/cat9k-rpboot.17.01.01.SPA.pkg
/flash/cat9k-sipbase.17.01.01.SPA.pkg
/flash/cat9k-sipspa.17.01.01.SPA.pkg
/flash/cat9k-srdriver.17.01.01.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.16.09.01.SSA.bin
/flash/packages.conf.00-

Do you want to remove the above files? [y/n]y
[R0]:
Deleting file flash:cat9k-cc_srdriver.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.17.01.01.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.16.10.01.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 Wed 20 Nov 14:16:29 PDT 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.12.01c.SPA.bin flash:

Destination filename [cat9k_iosxe.16.12.01c.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.12.01c.SPA.bin...
Loading /cat9k_iosxe.16.12.01c.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 20 Nov 2019 13:35:16 -07:00 cat9k_iosxe.16.12.01c.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.16.12.01c.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.16.12.01c.SPA.bin activate commit

install_add_activate_commit: START Wed 20 Nov 22:49:41 UTC 2019

*Nov 20 22:49:42.772: %IOSXE-5-PLATFORM: Switch 1 R0/0: Nov 20 22:49:42 install_engine.sh:
%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.12.01c.SPA.bininstall_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.12.01c.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.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.12.01.SPA.pkg

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

--- Starting Commit ---
Performing Commit on all members
[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.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
```

```
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-guestshell.16.12.01.SPA.pkg
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.12.01.SPA.pkg
Wed Nov 20 22:53:58 UTC 2019
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

install_rollback: START Wed 20 Nov 14:24:56 UTC 2019

This operation requires a reload of the system. Do you want to proceed? [y/n]
*Nov 20 14:24:57.555: %IOSXE-5-PLATFORM: R0/0: Nov 20 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.17.01.01.SPA.pkg
Current : rp 1 0 rp_boot cat9k-rpboot.17.01.01.SPA.pkg
Replacement: rp 0 0 rp_boot cat9k-rpboot.16.12.01.SPA.pkg
Replacement: rp 1 0 rp_boot cat9k-rpboot.16.12.01.SPA.pkg
Current : cc 0  0 cc_srdriver cat9k-cc_srdriver.17.01.01.SPA.pkg
Current : cc 0  0 cc cat9k-sipbase.17.01.01.SPA.pkg
Current : cc 0  0 cc_spa cat9k-sipspa.17.01.01.SPA.pkg
Current : cc 1  0 cc_srdriver cat9k-cc_srdriver.17.01.01.SPA.pkg
Current : cc 1  0 cc cat9k-sipbase.17.01.01.SPA.pkg
Current : cc 1  0 cc_spa cat9k-sipspa.17.01.01.SPA.pkg
Current : cc 10 0 cc cat9k-sipbase.17.01.01.SPA.pkg
Current : cc 10 0 cc_spa cat9k-sipspa.17.01.01.SPA.pkg
Current : cc 10 0 cc_srdriver cat9k-cc_srdriver.17.01.01.SPA.pkg
Current : cc 2  0 cc_srdriver cat9k-cc_srdriver.17.01.01.SPA.pkg
Current : cc 2  0 cc cat9k-sipbase.17.01.01.SPA.pkg
Current : cc 2  0 cc_spa cat9k-sipspa.17.01.01.SPA.pkg
Current : cc 3  0 cc_srdriver cat9k-cc_srdriver.17.01.01.SPA.pkg
Current : cc 3  0 cc cat9k-sipbase.17.01.01.SPA.pkg
Current : cc 3  0 cc_spa cat9k-sipspa.17.01.01.SPA.pkg
Current : cc 4  0 cc_srdriver cat9k-cc_srdriver.17.01.01.SPA.pkg
Current : cc 4  0 cc cat9k-sipbase.17.01.01.SPA.pkg
Current : cc 4  0 cc_spa cat9k-sipspa.17.01.01.SPA.pkg
Current : cc 5  0 cc_srdriver cat9k-cc_srdriver.17.01.01.SPA.pkg
Current : cc 5  0 cc cat9k-sipbase.17.01.01.SPA.pkg
Current : cc 5  0 cc_spa cat9k-sipspa.17.01.01.SPA.pkg
Current : cc 6  0 cc_srdriver cat9k-cc_srdriver.17.01.01.SPA.pkg
Current : cc 6  0 cc cat9k-sipbase.17.01.01.SPA.pkg
Current : cc 6  0 cc_spa cat9k-sipspa.17.01.01.SPA.pkg
Current : cc 7  0 cc_srdriver cat9k-cc_srdriver.17.01.01.SPA.pkg
Current : cc 7  0 cc cat9k-sipbase.17.01.01.SPA.pkg
Current : cc 7  0 cc_spa cat9k-sipspa.17.01.01.SPA.pkg
```

```
Current : cc 8  0 cc_srdriver cat9k-cc_srdriver.17.01.01.SPA.pkg
Current : cc 8  0 cc cat9k-sipbase.17.01.01.SPA.pkg
Current : cc 8  0 cc_spa cat9k-sipspa.17.01.01.SPA.pkg
Current : cc 9  0 cc_srdriver cat9k-cc_srdriver.17.01.01.SPA.pkg
Current : cc 9  0 cc cat9k-sipbase.17.01.01.SPA.pkg
Current : cc 9  0 cc_spa cat9k-sipspa.17.01.01.SPA.pkg
Current : fp 0  0 fp cat9k-espbase.17.01.01.SPA.pkg
Current : fp 1  0 fp cat9k-espbase.17.01.01.SPA.pkg
Current : rp 0  0 guestshell cat9k-guestshell.17.01.01.SPA.pkg
Current : rp 0  0 rp_base cat9k-rpbase.17.01.01.SPA.pkg
Current : rp 0  0 rp_daemons cat9k-rpbase.17.01.01.SPA.pkg
Current : rp 0  0 rp_iosd cat9k-rpbase.17.01.01.SPA.pkg
Current : rp 0  0 rp_security cat9k-rpbase.17.01.01.SPA.pkg
Current : rp 0  0 rp_webui cat9k-webui.17.01.01.SPA.pkg
Current : rp 0  0 rp_wlc cat9k-wlc.17.01.01.SPA.pkg
Current : rp 0  0 srdriver cat9k-srdriver.17.01.01.SPA.pkg
Current : rp 1  0 guestshell cat9k-guestshell.17.01.01.SPA.pkg
Current : rp 1  0 rp_base cat9k-rpbase.17.01.01.SPA.pkg
Current : rp 1  0 rp_daemons cat9k-rpbase.17.01.01.SPA.pkg
Current : rp 1  0 rp_iosd cat9k-rpbase.17.01.01.SPA.pkg
Current : rp 1  0 rp_security cat9k-rpbase.17.01.01.SPA.pkg
Current : rp 1  0 rp_webui cat9k-webui.17.01.01.SPA.pkg
Current : rp 1  0 rp_wlc cat9k-wlc.17.01.01.SPA.pkg
Current : rp 1  0 srdriver cat9k-srdriver.17.01.01.SPA.pkg
Replacement: cc 0  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Replacement: cc 0  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Replacement: cc 0  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Replacement: cc 1  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Replacement: cc 1  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Replacement: cc 1  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Replacement: cc 10 0 cc cat9k-sipbase.16.12.01.SPA.pkg
Replacement: cc 10 0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Replacement: cc 10 0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Replacement: cc 2  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Replacement: cc 2  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Replacement: cc 2  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Replacement: cc 3  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Replacement: cc 3  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Replacement: cc 3  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Replacement: cc 4  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Replacement: cc 4  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Replacement: cc 4  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Replacement: cc 5  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Replacement: cc 5  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Replacement: cc 5  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Replacement: cc 6  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Replacement: cc 6  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Replacement: cc 6  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Replacement: cc 7  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Replacement: cc 7  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Replacement: cc 7  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Replacement: cc 8  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Replacement: cc 8  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Replacement: cc 8  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Replacement: cc 9  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Replacement: cc 9  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Replacement: cc 9  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Replacement: fp 0  0 fp cat9k-espbase.16.12.01.SPA.pkg
Replacement: fp 1  0 fp cat9k-espbase.16.12.01.SPA.pkg
Replacement: rp 0  0 guestshell cat9k-guestshell.16.12.01.SPA.pkg
Replacement: rp 0  0 rp_base cat9k-rpbase.16.12.01.SPA.pkg
Replacement: rp 0  0 rp_daemons cat9k-rpbase.16.12.01.SPA.pkg
Replacement: rp 0  0 rp_iosd cat9k-rpbase.16.12.01.SPA.pkg
Replacement: rp 0  0 rp_security cat9k-rpbase.16.12.01.SPA.pkg
```

```
Replacement: rp 0  0 rp_webui cat9k-webui.16.12.01.SPA.pkg
Replacement: rp 0  0 srdriver cat9k-srdriver.16.12.01.SPA.pkg
Replacement: rp 1  0 guestshell cat9k-guestshell.16.12.01.SPA.pkg
Replacement: rp 1  0 rp_base cat9k-rpbase.16.12.01.SPA.pkg
Replacement: rp 1  0 rp_daemons cat9k-rpbase.16.12.01.SPA.pkg
Replacement: rp 1  0 rp_iosd cat9k-rpbase.16.12.01.SPA.pkg
Replacement: rp 1  0 rp_security cat9k-rpbase.16.12.01.SPA.pkg
Replacement: rp 1  0 rp_webui cat9k-webui.16.12.01.SPA.pkg
Replacement: rp 1  0 srdriver cat9k-srdriver.16.12.01.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 Wed 20 Nov 14:26:35 UTC 2019

Switch#
*Mar 06 14:26:35.880: %IOSXE-5-PLATFORM: R0/0: Mar 06 14:26:35 install_engine.sh:
%INSTALL-5-INSTALL_COMPLETED_INFO: Completed install rollback PACKAGE
*Mar 06 14:26:37.740: %IOSXE_OIR-6-REMCARD: Card (rp) removed from slot R1
*Mar 06 14:26:39.253: %IOSXE_OIR-6-INSCARD: Card (rp) inserted in slot R1Nov 2 14:26:5

Initializing Hardware...

System Bootstrap, Version 16.12.1r, RELEASE SOFTWARE (P)
Compiled Mon 07/22/2019 10:19:23.77 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-19 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 switch 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 Gibraltar 16.12.1c image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.12.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.12.1c, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Wed 20-Nov-19 10:48 by mcpre
<output truncated>
```

Upgrading the Complex Programmable Logic Device Version

You can trigger a CPLD version upgrade after upgrading the software image. During CPLD upgrade, the supervisor module automatically power cycles which may cause a temporary loss of uplink connectivity. This completes the CPLD upgrade process for the supervisor module. Auto-upgrade of CPLD is not supported, and so you must manually perform CPLD upgrade.

Upgrading the CPLD Version: High Availability Setup

Beginning in the privileged EXEC mode, complete the following steps:

Before you begin

When performing the CPLD version upgrade as shown, the **show platform** command can be used to confirm the CPLD version after the upgrade. This command output shows the CPLD version on all modules. However, the CPLD upgrade only applies to the supervisors, not the line cards. The line cards CPLD version is a cosmetic display. After the upgrade is completed in a high availability setup, the supervisors will be upgraded, but the line cards will still show the old CPLD version. The version mismatch between the supervisors and line cards is expected until a chassis reload.

Procedure

Step 1 Upgrade the CPLD Version of the standby supervisor module

Enter the following commands on the active supervisor:

a) `Device# configure terminal`
b) `Device(config)# service internal`
c) `Device(config)# exit`
d) `Device# upgrade hw-programmable cpld filename bootflash: rp standby`

The standby supervisor module reloads automatically and the upgrade occurs in ROMMON. During the upgrade, the supervisor module automatically power cycles and remains inactive for approximately 5 minutes.

Wait until the standby supervisor module boots up and the SSO has formed (HOT) before you proceed to the next step; this takes approximately 17 minutes.

Step 2 Perform a switch over

a) `Device# redundancy force-switchover`

This causes the standby supervisor (on which you have completed the CPLD upgrade in Step 1) to become the active supervisor module

Step 3 Upgrade the CPLD Version of the new standby supervisor module

Repeat Step 1 and all its substeps.

Note
Do not operate an HA system with mismatched FPGA versions. FPGA version should be upgraded on both the supervisors one at a time.

Upgrading the CPLD Version: Cisco StackWise Virtual Setup

Beginning in the privileged EXEC mode, complete the following steps:

Procedure

Step 1 Upgrade the CPLD version of the standby supervisor module

Enter the following commands on the active supervisor:

a) `Device# configure terminal`
b) `Device(config)# service internal`
c) `Device(config)# exit`
d) `Device# upgrade hw-programmable cpld filename bootflash: switch standby [r0 | r1]`

Use **r0** if the targeted Supervisor is on the lower slot of the chassis, and **r1** if the targeted Supervisor is on the upper slot of the chassis.

Note
For the **upgrade hw-programmable cpld filename bootflash** command, configure with the **switch** keyword only. The other available keywords are not applicable when upgrading with Cisco StackWise Virtual.

Step 2 Reload the standby supervisor module

a) `Device# redundancy reload peer`

The upgrade occurs in ROMMON. During the upgrade, the supervisor module automatically power cycles and remains inactive for approximately 5 minutes.

Wait until the standby supervisor module boots up and the SSO has formed (HOT) before you proceed to the next step; this takes approximately 17 minutes.

Step 3 Perform a switch over

a) `Device# redundancy force-switchover`

This causes the standby supervisor (on which you have completed the CPLD upgrade in step 1) to become the active supervisor module

Step 4 Upgrade the CPLD version of the new standby supervisor module

Perfom Steps 1 and 2, including all substeps, on the new standby supervisor module

Upgrading the CPLD Version: Single Supervisor Module Setup

Beginning in the privileged EXEC mode, complete the following steps:

Procedure

Upgrade the CPLD version of the active supervisor module

Enter the following commands on the active supervisor:

a) `Device# configure terminal`
b) `Device(config)# service internal`
c) `Device(config)# exit`
d) `Device# upgrade hw-programmable cpld filename bootflash: rp active`

The supervisor module reloads automatically and the upgrade occurs in ROMMON. During the upgrade, the supervisor module automatically power cycles and remains inactive for approximately 5 minutes.

Licensing

For information about licenses required for the features available on Cisco Catalyst 9000 Series Switches, see Configuring Licenses on Cisco Catalyst 9000 Series Switches.

All licensing information relating to Cisco Catalyst 9000 Series Switches are available on this collection page: Cisco Catalyst 9000 Switching Family Licensing.

Available Licensing Models and Configuration Information

- Cisco IOS XE Fuji 16.8.x and earlier: RTU Licensing is the default and the only supported method to manage licenses.
- Cisco IOS XE Fuji 16.9.1 to Cisco IOS XE Amsterdam 17.3.1: Smart Licensing is the default and the only supported method to manage licenses.
- Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy, which is an enhanced version of Smart Licensing, is the default and the only supported method to manage licenses.

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

- 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.
- Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
- 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 layer 2 port-channels, 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.
- In-Service Software Upgrade (ISSU)
  - ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.10.x or to Cisco IOS XE Gibraltar 16.11.x is not supported. This applies to both a single and dual supervisor module setup.
  - While performing ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.12.x, if **interface-id snmp-if-index** command is not configured with OSPFv3, packet loss can occur. Configure the **interface-id snmp-if-index** command either during the maintenance window or after isolating the device (by using maintenance mode feature) from the network before doing the ISSU.
  - While ISSU allows you to perform upgrades with zero downtime, we recommend you to do so during a maintenance window only.
  - If a new feature introduced in a software release requires a change in configuration, the feature should not be enabled during ISSU.
  - If a feature is not available in the downgraded version of a software image, the feature should be disabled before initiating ISSU.
- 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.
  - Stack Queuing and Scheduling (SQS) drops CPU bound packets exceeding 1.4 Gbps.

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

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

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

- VLAN Restriction—It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.
- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.
- Embedded Event Manager—Identity event detector is not supported on Embedded Event Manager.
- The File System Check (fsck) utility is not supported in install mode.
- Switch Web UI allows configuration of data VLANs only and not voice VLANs. If you remove a voice VLAN configured to an interface using the Web UI, then all data VLANs associated with the interface are also removed by default.

Caveats

Caveats describe unexpected behavior in Cisco IOS-XE releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat, click on the identifier.

Open Caveats in Cisco IOS XE Amsterdam 17.1.x

Identifier	Description
CSCvq72472	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvr43553	C9400-LC-24XS LC went into faulty state with few ports in err-disabled state, after chassis reload
CSCvr88026	C9407R Power setting, default to combine after reload

Identifier	Description
CSCvr90237	Mulitple issues seen if we do SSO with MKA MACsec on Sup ports.
CSCvr92287	EPC with packet-len opt breaks CPU in-band path for bigger frames
CSCvr92660	STP BPDUs not being sent from FED to IOSd
CSCvr98281	After valid ip conflict, SVI admin down responds to GARP
CSCvr99132	SPANed multicast packet reduced TTL
CSCvs00513	iomd crash and LCs in faulty states after autoLC shutdown and config shut/no shut
CSCvs14893	802.1x-MultiAuth/MultiDomain: C9K - Traffic drop in egress direction for Data-Vlan on a Auth port

Resolved Caveats in Cisco IOS XE Amsterdam 17.1.1

Identifier	Description
CSCvo36359	C9400: Enable TestUnusedPortLoopback.
CSCvo66246	Enabling SPAN source of VLAN 1 affects LACP operations
CSCvp62101	C9400 ~3sec Traffic Loss on Uplink Port Channel After Active SUP removal
CSCvp84502	ERSPAN destination does not work or forward traffic
CSCvq13053	NAT translation entry not cleared after fin-rst time-out
CSCvq22224	cat9k // evpn/vxlan // dhcp relay not working over l3vni
CSCvq30460	SYS-2-BADSHARE: Bad refcount in datagram_done - messages seen during system churn
CSCvq30464	CAT9400: MTU config not getting applied to inactive ports becoming active
CSCvq40137	Mac address not being learnt when "auth port-control auto" command is present
CSCvq43450	C9400 Sup uplinks with netflow configuration stopped forwarding traffic after switchover
CSCvq58991	C9400/16.11.1 - Diagnostic test of TestPortTxMonitoring is failing for DAD links
CSCvq72713	Cat3k/Cat9k can't forwarding traffic follow the rule of EIGRP unequal cost load-balancing
CSCvq93773	C9600/9400/9500H/9300 etc crashes due to CMCC heartbeat failures
CSCvr04551	Multicast stream flickers on igmp join/leave
CSCvr04660	change show module output from faulty to post-fail for post failures
CSCvr07162	system crash on execute "fed TCAM utilization"

Identifier	Description
CSCvr29921	Inserting 1Gige SFP (GLC-SX-MMD or SFP GE-T) to SUP port causes another port to link flap.
CSCvr43959	C9400 ISSU to 16.9.4 or 16.12.1c With Port Security Enabled Causes Traffic Loss
CSCvr46931	ports remain down/down object-manager (fed-ots-mo thread is stuck)
CSCvr82402	SNMP timeout when querying entSensorValueEntry

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 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: 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 DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

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

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

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

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

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

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

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

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

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

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

© 2019 Cisco Systems, Inc. All rights reserved.