Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Everest 16.6.x

First Published: July 31, 2017
Last Updated: March 01, 2021

This release note gives an overview of the hardware and software with the Cisco IOS XE Everest 16.6.x, on the Cisco Catalyst 9400 Series Switches.

- For information about unsupported features, see Important Notes, page 8
- For information about software and hardware restrictions and limitations, see Limitations and Restrictions, page 33.
- For information about open issues with the software, see Caveats, page 34.

Introduction

Cisco Catalyst 9400 Series Switches are Cisco's leading modular enterprise switching access platform built for security, IoT and Cloud.

Cisco Catalyst 9400 Series Switches deliver complete convergence in terms of ASIC architecture with a Unified Access Data Plane (UADP) 2.0. The series forms the foundational building block for Software Defined-Access (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 Everest 16.6.10

There are no new hardware or software features in this release.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Whats New in Cisco IOS XE Everest 16.6.9

There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.8

There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.7

There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.6

There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.5

There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.4a

There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.4

There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.3

Software Features in Cisco IOS XE Everest 16.6.3

Feature Name	Description and License Level Information
Software Maintenance Upgrade (SMU)	SMU is a package that can be installed on a system, to provide a patch fix or security resolution to a released image. See System Management -> Software Maintenance Upgrade. (DNA Advantage)
Show commands	The output for **show inventory** and **show id prom fan-tray** commands is enhanced to display the Chassis serial number of the fan-tray along with the existing PCB Serial Number. See System Management Commands.

Whats New in Cisco IOS XE Everest 16.6.2

Hardware Features in Cisco IOS XE Everest 16.6.2

Feature Name	Description and License Level Information
C9400-LC-24XS	Cisco Catalyst 9400 Series 24-Port SFP/SFP+ Module See Cisco Catalyst 9400 Series Switching Module Installation Note.
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) UPOE Multigigabit See Cisco Catalyst 9400 Series Switching Module Installation Note.
C9400-SUP-1XL	Cisco Catalyst 9400 Series Supervisor 1XL Module This supervisor module is supported on C9407R, C9410R chassis. See Cisco Catalyst 9400 Series Supervisor Module Installation Note.

Software Features in Cisco IOS XE Everest 16.6.2

Feature Name	Description and License Level Information
New in Wired Switching	
Bidirectional Forwarding Detection	Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. (Network Essentials)
Cisco Discovery Protocol Bypass	A backward compatible mode, equivalent to not having Cisco Discovery Protocol support. When the feature is enabled, Cisco Discovery Protocol packets are received and transmitted unchanged. Received packets are not processed; no packets are generated. In this mode, 'bump-in-the-wire' behavior is applied to Cisco Discovery Protocol packets. See Security -> Cisco Discovery Protocol Bypass. (Network Essentials and Network Advantage)

EIGRP BFD	The EIGRP-BFD Support feature helps configure the Enhanced Interior Gateway Routing Protocol (EIGRP) with Bidirectional Forwarding Detection (BFD) so that EIGRP registers with BFD and receives all forwarding path detection failure messages from BFD. (Network Essentials)
Encrypted Traffic Analytics (ETA)	Studies the packet flow behavior of an application to determine the flow characteristics such as, malware analysis, and crypto audit. See Network Management -> Configuring Encrypted Traffic Analytics. (DNA Advantage)
Nonstop Forwarding with Stateful Switchover	The switch supports high availability or stateful switchover (SSO) by allowing a redundant supervisor engine to take over if a primary supervisor engine fails. Stateful switchover minimizes the time a network is unavailable to users following a switchover, while continuing to forward IP packets. The user session information is maintained during a switchover, and line cards continue to forward network traffic with no loss of sessions. See NSF with SSO. Nonstop Forwarding (Network Advantage) Stateful Switchover (Network Essentials)
Software-Defined Access (SDA)	Provides the basic infrastructure for building virtual networks on policy-based segmentation constructs. It is based on Locator ID Separator Protocol (LISP) overlay network built on top of an arbitrary underlay network. Cisco IOS XE Everest 16.6.2 supports Layer 2 and Layer 3 overlay networks. This release introduces support for wireless devices on fabric edge nodes. You can now connect traditional Layer 2 networks, wireless access points, or end hosts to the fabric edge nodes. See *Campus Fabric* (Network Advantage)

Multiprotocol Label Switching • MPLS EM—MPLS Multipath (ECMP) LSP Tree Trace • MPLS Label Distribution Protocol (LDP) • MPLS LDP—Graceful Restart • MPLS LDP—Inbound Label Binding Filtering • MPLS LDP—Session Protection • MPLS Static Labels • MPLS Traceroute • MPLS Virtual Private Networks (VPNs) – MPLS VPN ID	The following MPLS features are introduced in this release: • MPLS—Combines the performance and capabilities of Layer 2 (data link layer) switching with the proven scalability of Layer 3 (network layer) routing. • MPLS Multipath LSP Tree Trace—Provides the means to discover all possible equal-cost multipath (ECMP) routing paths of a label switched path (LSP) between an egress and ingress router. Once discovered, these paths can be retested on a periodic basis using MPLS LSP ping or traceroute. • MPLS LDP—This protocol supports MPLS hop-by-hop forwarding by distributing bindings between labels and network prefixes. • MPLS LDP Graceful Restart—Assists a neighboring device that has MPLS LDP Stateful Switchover/Nonstop Forwarding (SSO/NSF) Support and Graceful Restart to recover gracefully from an interruption in service. • MPLS LDP Inbound Label Binding Filtering—MPLS LDP Inbound Label Binding Filtering helps to configure access control lists (ACLs) for controlling the label bindings a label switch router (LSR) accepts from its peer LSRs. • MPLS LDP Session Protection—Provides faster label distribution protocol convergence when a link recovers following an outage. MPLS LDP Session Protection protects an LDP session between directly connected neighbors or an LDP session established for a traffic engineering (TE) tunnel. • MPLS Static Labels—MPLS Static Labels provides the means to configure statically: – The binding between a label and an IPv4 prefix. – The contents of an LFIB crossconnect entry. • MPLS Traceroute—Helps service providers monitor label switched paths (LSPs) and quickly isolate MPLS forwarding problems. • MPLS VPN ID—Helps identify VPNs by a VPN identification number, as described in RFC 2685. The MPLS VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with MPLS VPN ID numbers in routing updates. See Multiprotocol Label Switching (MPLS). (Network Advantage)

Programmability • Zero-Touch Provisioning (ZTP) • Guest Shell • Preboot Execution Environment Client (iPXE) • Python APIs • Python CLI Module • EEM Python Module • NETCONF Programmable Interface • Model-Driven Telemetry • YANG Data Models • In-Service Model Updates	Programmability features introduced or enhanced in this release: • ZTP—Zero-Touch Provisioning automates the process of installing or upgrading software images, and installing configuration files on Cisco devices that are deployed in a network for the first time. It reduces manual tasks required to scale the network capacity. It also supports HTTP file download along with TFTP file download. (Network Essentials) • Guest Shell is a virtualized Linux-based environment, designed to run custom Linux applications, including Python for automated control and management of Cisco devices. It also includes the automated provisioning (Day zero) of systems. (DNA Essentials) • iPXE—An open Preboot eXecution Environment (PXE) client that allows a device to boot from a network boot image. iPXE is supported with IPv4 only. (Network Essentials) • Python APIs—Python programmability supports Python APIs. (DNA Essentials) • Python CLI Module—Python Programmability provides a Python module that allows users to interact with IOS using CLIs. (DNA Essentials) • EEM Python Module—Embedded Event Manager (EEM) policies support Python scripts. Python scripts can be executed as part of EEM actions in EEM applets. (DNA Essentials) • NETCONF—provides a simpler mechanism to install, manipulate, and delete the configuration of network devices. It uses an Extensible Markup Language (XML)-based data encoding for the configuration data as well as the protocol messages. (Network Essentials) • Model-Driven Telemetry—Provides a mechanism to stream data from a Model-Driven Telemetry-capable device, to a destination. The data to be streamed is driven through subscription. The feature is enabled automatically, when NETCONF-YANG is started on a device. (Network Essentials) • 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/1662. (Network Essentials) 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. • In-Service Model Updates—Adds new data models or extend functionality to existing data models. The In Service Model Update provides YANG model enhancements outside of a release cycle. (Network Essentials) See the Programmability Configuration Guide, Cisco IOS XE Everest 16.6.x.

Important Notes

The following are the unsupported hardware and software features for the Cisco Catalyst 9400 Series Switches. For the list of supported features, go to http://www.cisco.com/go/cfn.

Unsupported hardware features

- The SFP or SFP+ port set-enabled LED remain off on the supervisor module. They remain Off even if the SFP or SFP+ ports are enabled.

Unsupported software features

- Audio Video Bridging (including IEEE802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav)
- Bluetooth
- Boot Integrity Visibility
- 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
- IPsec with FIPS
- MACSec Encryption—Both host link encryption (downlinks) and inter network device encryption (uplinks), with 128-bit and 256-bit AES MACsec (IEEE 802.1AE)
- Network-Powered Lighting (including COAP Proxy Server, 2-event Classification, Perpetual POE, Fast PoE)
- VRF Aware Web-Authentication

Supported Hardware

Supported Cisco Catalyst 9400 Series Switches

For information about the available license levels, see section License Levels, page 31.

Table 1 Supported Switch Models

Product ID (PID) (append with "=" for spares)	Description
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

Table 2 Supported Hardware on Cisco Catalyst 9400 Series Switches

Product ID (append with "=" for spares)	Description
Supervisor Engines	
C9400-SUP-1	Cisco Catalyst 9400 Series Supervisor 1 Module This supervisor module is supported on C9407R, C9410R chassis
C9400-SUP-1XL	Cisco Catalyst 9400 Series Supervisor 1XL Module This supervisor module is supported on C9407R, C9410R chassis
Gigabit Ethernet Switching Modules	
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)
TenGigabit Ethernet Switching Modules	
C9400-LC-24XS	Cisco Catalyst 9400 Series 24-Port SFP/SFP+ Module
Multigigabit Ethernet Switching Modules	

Table 2 Supported Hardware on Cisco Catalyst 9400 Series Switches

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) UPOE Multigigabit (mGig)
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
Power Supply Modules	
C9400-PWR-3200AC	Cisco Catalyst 9400 Series 3200W AC Power Supply

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

Optics Modules

Catalyst switches support a wide range of optics. Because the list of supported optics is updated on a regular basis, consult the tables at this URL for the latest compatibility information:

http://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html

Compatibility Matrix

Table 3 Software Compatibility Matrix

Catalyst 9400	Cisco Identity Services Engine	Cisco Access Control Server	Prime Infrastructure
Everest 16.6.10	2.4	5.4 5.5	PI 3.9 See Prime Infrastructure 3.9 on cisco.com
Everest 16.6.9	2.4	5.4 5.5	PI 3.9 See Prime Infrastructure 3.9 on cisco.com
Everest 16.6.8	2.4	5.4 5.5	PI 3.8 See Prime Infrastructure 3.8 on cisco.com
Everest 16.6.7	2.2 2.3 2.4	5.4 5.5	PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.
Everest 16.6.6	2.2 2.3 2.4	5.4 5.5	PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.

Table 3 Software Compatibility Matrix

Catalyst 9400	Cisco Identity Services Engine	Cisco Access Control Server	Prime Infrastructure
Everest 16.6.5	2.2 2.3 2.4	5.4 5.5	PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.
Everest 16.6.4a	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.
Everest 16.6.4	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.
Everest 16.6.3	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.
Everest 16.6.2	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.
Everest 16.6.1	2.2	5.4 5.5	PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.

Web UI System Requirements

The following sections list the hardware and software required to access the Web UI:

Hardware Requirements

Table 4 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1. We recommend 1 GHz.
2. 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 and later (On Windows and Mac)
- Microsoft Internet Explorer—Version 11 or later (On Windows 7 and Windows XP), and Microsoft Edge (On Windows 10)
- Mozilla Firefox—Version 33 and later (On Windows and Mac)
- Safari—Version 7 and later (On Mac)

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.

Table 5 Software Images

Release	Image	File Name
Cisco IOS XE Everest 16.6.10	CAT9K_IOSXE	cat9k_iosxe.16.06.10.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.06.10.SPA.bin
Cisco IOS XE Everest 16.6.9	CAT9K_IOSXE	cat9k_iosxe.16.06.09.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.06.09.SPA.bin
Cisco IOS XE Everest 16.6.8	CAT9K_IOSXE	cat9k_iosxe.16.06.08.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.06.08.SPA.bin
Cisco IOS XE Everest 16.6.7	CAT9K_IOSXE	cat9k_iosxe.16.06.07.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.06.07.SPA.bin
Cisco IOS XE Everest 16.6.6	CAT9K_IOSXE	cat9k_iosxe.16.06.06.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.06.06.SPA.bin
Cisco IOS XE Everest 16.6.5	CAT9K_IOSXE	cat9k_iosxe.16.06.05.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.06.05.SPA.bin
Cisco IOS XE Everest 16.6.4a	CAT9K_IOSXE	cat9k_iosxe.16.06.04a.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.06.04a.SPA.bin

Table 5 Software Images (continued)

Release	Image	File Name
Cisco IOS XE Everest 16.6.4	CAT9K_IOSXE	cat9k_iosxe.16.06.04.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.06.04.SPA.bin
Cisco IOS XE Everest 16.6.3	CAT9K_IOSXE	cat9k_iosxe.16.06.03.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.06.03.SPA.bin
Cisco IOS XE Everest 16.6.2	CAT9K_IOSXE	cat9k_iosxe.16.06.02.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.06.02.SPA.bin
Cisco IOS XE Everest 16.6.1	CAT9K_IOSXE	cat9k_iosxe.16.06.01.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.06.01.SPA.bin

Upgrading the Switch Software

Note You cannot use the Web UI to install, upgrade, or downgrade switch software

This section covers the following:

- Automatic Boot Loader Upgrade and CPLD Upgrade
- Upgrading in Install Mode
- Downgrading in Install Mode

Table 6 install commands to Upgrade or Downgrade Switch Software

Switch# **install add file** *filename* [**activate commit**]—Use this command to install and activate the specified file, and to commit changes to be persistent across reloads.	
Switch# **install ?** —You can also use the **install** command to separately install, activate, commit, cancel, or remove the installation file.	
add file *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 the image activation.
commit	Makes changes persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels the 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.

Automatic Boot Loader Upgrade and CPLD Upgrade

Note If you are upgrading from Cisco IOS XE Everest 16.6.2 to 16.6.3 or 16.6.4, 16.6.4a,16.6.5 there is no ROMMON or CPLD firmware upgrade.
In case of upgrade from Cisco IOS XE Everest 16.6.1 to 16.6.3 or 16.6.4, there will be a ROMMON and CPLD upgrade.

Automatic Boot Loader Upgrade

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

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

During an upgrade, reload is not required; the system will auto reload, and the new ROMMON image will be available.

When upgrading from IOS XE Everest 16.6.1 to 16.6.2, 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 IOS XE Everest 16.6.2.

Note If Catalyst 9400 Supervisor1 power is removed and reapplied within a 5-second window, the boot SPI may get corrupted.

When upgrading from IOS XE Everest 16.6.1 to 16.6.2, for the first time, 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. Once both supervisors are upgraded to IOS XE16.6.2, they can be inserted in high availability setup.

Note Do not upgrade dual supervisors from IOS XE Everest 16.6.1 to 16.6.2 at the same time to avoid hardware damage.

Caution Do not power cycle your switch during the upgrade.

Table 7 Automatic Boot Loader Response

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE Everest 16.6.2,
or Cisco IOS XE Everest 16.6.3,
or Cisco IOS XE Everest 16.6.4,
or Cisco IOS XE Everest 16.6.4a,
or Cisco IOS XE Everest 16.6.5,
or Cisco IOS XE Everest 16.6.6,
or Cisco IOS XE Everest 16.6.7,
or Cisco IOS XE Everest 16.6.8,
or Cisco IOS XE Everest 16.6.9,
or Cisco IOS XE Everest 16.6.10
for the first time
	The boot loader may be upgraded to version 16.6.2r [FC1]. For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 16.6.2r [FC1], RELEASE SOFTWARE (P)`
	If the automatic boot loader upgrade occurs while booting, you will see the following on the console:
	`%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Fri Nov 03 18:42:58 Universal 2017 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): boot loader upgrade successful`
	`%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): Reloading the Supervisor to enable the New BOOTLOADER`

If you boot Cisco IOS XE Everest 16.6.1 the first time	The boot loader may be upgraded to version 16.6.1r [FC2]. For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 16.6.1r [FC2], RELEASE SOFTWARE`
	If the automatic boot loader upgrade occurs while booting Cisco IOS XE Everest 16.6.1, you will see the following on the console:
	`%IOSXEBOOT-Wed-###: (rp/0): Jul 26 16:57:44 Universal 2017 PLEASE DO NOT POWER CYCLE ###BOOT LOADER UPGRADING 4`
	`Both links down, not waiting for other switches`
	`Switch number is 1`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful 4`

CPLD Upgrade

During the automatic boot loader upgrade, mcnewfpgaclose.hdr and mcnewfpgaclose.img are copied to the bootflash. The supervisor automatically reloads to enable the new boot loader.

When the new boot loader boots up, the complex programmable logic device (CPLD) upgrade process starts automatically. The CPLD upgrade process will take approximately from 7 to 10 minutes. The supervisor will power cycle itself during the CPLD upgrade.

Caution Do not unplug power or remove the supervisor during the upgrade.

The following is sample output from 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
```

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**."

Note This procedure automatically copies the images to both active and standby supervisors. Both supervisors are simultaneously upgraded. In Cisco IOS XE Everest 16.6.1, the upgrade will not occur for standby supervisor as dual-supervisor is not supported in this release.

The sample output in this section covers upgrade from Cisco IOS XE Everest 16.6.1 to Cisco IOS XE Everest 16.6.2 in Install Mode. The same sample output will be applicable to Cisco IOS XE Everest 16.6.3 and later releases on the Cisco IOS XE Everest 16.6.x release train.

Summary Steps—Clean Up > Copy New Image to Flash > Software Install Image to Flash > Reload

Clean Up

Step 1 Ensure that you have at least 1GB of space in flash to expand a new image. Clean up old installation files in case of insufficient space.

```
Switch# install remove inactive

install_remove: START Tue Jun 20 14:14:40 PDT 2017
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.16.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-espbase.16.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpbase.16.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpboot.16.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipbase.16.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipspa.16.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-srdriver.B16.06.01.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.16.06.01.SPA.pkg
/flash/cat9k-espbase.16.06.01.SPA.pkg
/flash/cat9k-rpbase.16.06.01.SPA.pkg
/flash/cat9k-rpboot.16.06.01.SPA.pkg
/flash/cat9k-sipbase.16.06.01.SPA.pkg
/flash/cat9k-sipspa.16.06.01.SPA.pkg
/flash/cat9k-srdriver.16.06.01.SPA.pkg
```

```
/flash/cat9k-webui.16.06.01.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.16.06.01.SSA.bin
/flash/packages.conf.00-

Do you want to remove the above files? [y/n]y
[R0]:
Deleting file flash:cat9k-cc_srdriver.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.01.SPA.pkg ... done.
Deleting file
Deleting file flash:cat9k-rpbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.B16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.01.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.16.06.01.SSA.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#
```

Copy New Image to Flash

Step 2 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 - 601216545 bytes]

601216545 bytes copied in 50.649 secs (11870255 bytes/sec)
```

Use the **dir flash** command to confirm that the image has been successfully copied to flash.

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

Directory of flash:/

434184  -rw- 601216545 Jul 26 2017 10:18:11 -07:00 cat9k_iosxe.16.06.02.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

Software Install Image to Flash

Step 3 Use the **install add file activate commit** 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.16.06.02.SPA.bin activate commit

install_add_activate_commit: START Fri Jun  9 22:49:41 UTC 2017
*Jun  9 22:49:42.772: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jun  9 22:49:42
install_engine.sh: %INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.06.02.SPA.bin
install_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-guestshell.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 Jun  9 22:53:58 UTC 2017
Switch#
```

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

Step 4 After the software has been successfully installed, verify that the flash partition has nine new .pkg files and three .conf files. See sample output below.

```
Switch# dir flash:*.pkg

Directory of flash:/*.pkg

Directory of flash:/
253956  -rw-   2097152 Nov 3  2017 21:37:04  -07:00 nvram_config
253955  -rw-   2097152 Nov 3  2017 21:37:04  -07:00 nvram_config_bkup
253954  -rw-       239 Nov 3  2017 21:28:47  -07:00 boothelper.log
253957  -rw-        78 Oct 27 2017 14:28:43  -07:00 tam_client_app.log
303110  -rw-   5297096 Nov 1  2017 23:27:26  -07:00 cat9k-cc_srdriver.16.06.01.SPA.pkg
253961  -rw-      7523 Nov 1  2017 23:56:25  -07:00 packages.conf
344067  -rw-   5186504 Nov 1  2017 23:54:10  -07:00 cat9k-cc_srdriver.16.06.02.SPA.pkg
303111  -rw-  80946116 Nov 1  2017 23:27:29  -07:00 cat9k-espbase.16.06.01.SPA.pkg
303112  -rw-   1536964 Nov 1  2017 23:27:29  -07:00 cat9k-guestshell.16.06.01.SPA.pkg
303113  -rw- 376865728 Nov 1  2017 23:27:40  -07:00 cat9k-rpbase.16.06.01.SPA.pkg
303118  -rw-  29545049 Nov 1  2017 23:27:53  -07:00 cat9k-rpboot.16.06.01.SPA.pkg
303114  -rw-  27669444 Nov 1  2017 23:27:41  -07:00 cat9k-sipbase.16.06.01.SPA.pkg
294913  drwx      4096 Nov 3  2017 21:28:25  -07:00 installer
253966  -rw-     16280 Nov 3  2017 21:28:42  -07:00 bootloader_evt_handle.log
303105  drwx      4096 Oct 26 2017 20:57:12  -07:00 core
311297  drwx      4096 Nov 2  2017 23:41:45  -07:00 prst_sync
327681  drwx      4096 Nov 1  2017 23:56:42  -07:00 rollback_timer
335873  drwx      4096 Nov 3  2017 21:28:46  -07:00 dc_profile_dir
335875  drwx      4096 Oct 26 2017 20:48:50  -07:00 gs_script
253959  -rw-       556 Nov 2  2017 23:42:12  -07:00 vlan.dat
253968  -rw-     98869 Nov 3  2017 21:28:59  -07:00 memleak.tcl
294914  drwx      4096 Oct 26 2017 21:19:34  -07:00 tech_support
303107  drwx      4096 Oct 26 2017 21:27:19  -07:00 onep
319490  drwx      4096 Oct 26 2017 21:27:19  -07:00 CRDU
303115  -rw-  55440320 Nov 1  2017 23:27:43  -07:00 cat9k-sipspa.16.06.01.SPA.pkg
303116  -rw-  11813828 Nov 1  2017 23:27:43  -07:00 cat9k-srdriver.16.06.01.SPA.pkg
303117  -rw-  12248000 Nov 1  2017 23:27:43  -07:00 cat9k-webui.16.06.01.SPA.pkg
344068  -rw-  76649412 Nov 1  2017 23:54:13  -07:00 cat9k-espbase.16.06.02.SPA.pkg
344069  -rw-   1536964 Nov 1  2017 23:54:13  -07:00 cat9k-guestshell.16.06.02.SPA.pkg
344070  -rw- 380625856 Nov 1  2017 23:54:24  -07:00 cat9k-rpbase.16.06.02.SPA.pkg
344076  -rw-  29580684 Nov 1  2017 23:54:39  -07:00 cat9k-rpboot.16.06.02.SPA.pkg
344071  -rw-  27612100 Nov 1  2017 23:54:24 -07:00  cat9k-sipbase.16.06.02.SPA.pkg
344072  -rw-  54981568 Nov 1  2017 23:54:26 -07:00  cat9k-sipspa.16.06.02.SPA.pkg
344073  -rw-   6521796 Nov 1  2017 23:54:26 -07:00  cat9k-srdriver.16.06.02.SPA.pkg
344074  -rw-  12268480 Nov 1  2017 23:54:26 -07:00  cat9k-webui.16.06.02.SPA.pkg
344075  -rw-   1536960 Nov 1  2017 23:54:26 -07:00  cat9k-wlc.16.06.02.SPA.pkg
344066  -rw-      7523 Nov 1  2017 23:54:39 -07:00  cat9k_iosxe.16.06.02.SPA.conf
253960  -rw-      7406 Nov 1  2017 23:56:25 -07:00  packages.conf.00-
11353194496 bytes total (9544245248 bytes free)
```

In the following sample output that 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.16.06.02.SPA.conf— a copy of packages.conf and not used by the system.

```
Switch# dir flash:*.conf

Directory of flash:/*.conf

Directory of flash:/
253961  -rw-      7523 Nov 1  2017 23:56:25 -07:00 packages.conf
344066  -rw-      7523 Nov 1  2017 23:54:39 -07:00 cat9k_iosxe.16.06.02.SPA.conf
253960  -rw-      7406 Nov 1  2017 23:56:25 -07:00 packages.conf.00-
11353194496 bytes total (8963174400 bytes free)
```

Reload

Step 5 Reload the switch

```
Switch# reload
```

Step 6 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
```

Step 7 When the new image boots up, verify the version of the new image, using the **show version** command:

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

```
Switch# show version

Cisco IOS XE Software, Version 16.06.02
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 Wed 01-Nov-17 07:26 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.

ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 16.6.2r[FC1], RELEASE SOFTWARE (P)

Switch uptime is 7 hours, 36 minutes
Uptime for this control processor is 7 hours, 24 minutes
System returned to ROM by SSO Switchover
System image file is "flash:packages.conf"
```

```
Last reload reason: redundancy force-switchover

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.

Technology Package License Information:
------------------------------------------------------------------
Technology-package                  Technology-package
Current             Type            Next reboot
------------------------------------------------------------------
network-essentials  Evaluation      network-essentials

cisco C9407R (X86) processor (revision V00) with 869104K/6147K bytes of memory.
Processor board ID FXS2119Q2U7
1 Virtual Ethernet interface
96 Gigabit Ethernet interfaces
88 Ten Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
15958488K 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:.

Configuration register is 0x102
Switch#
```

Downgrading in Install Mode

Note New hardware introduced in this release cannot be downgraded, so we recommend upgrading all existing switches to Cisco IOS XE Everest 16.6.2. For the list of models introduced in this release, see Hardware Features in Cisco IOS XE Everest 16.6.2

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**."

The sample output in this section covers downgrade from Cisco IOS XE Everest 16.6.2 to Cisco IOS XE Everest 16.6.1 in Install Mode.

Summary Steps—Clean Up > Copy New Image to Flash > Downgrade Software Image > Reload

Clean Up

Step 1 Ensure that you have at least 1GB of space in flash to expand a new image. Clean up old installation files in case of insufficient space.

```
Switch# install remove inactive

install_remove: START Tue Jun 20 14:14:40 PDT 2017
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.16.06.02.SPA.pkg
      File is in use, will not delete.
    cat9k-espbase.16.06.02.SPA.pkg
      File is in use, will not delete.
    cat9k-guestshell.16.06.02.SPA.pkg
      File is in use, will not delete.
    cat9k-rpbase.16.06.02.SPA.pkg
      File is in use, will not delete.
    cat9k-rpboot.16.06.02.SPA.pkg
      File is in use, will not delete.
    cat9k-sipbase.16.06.02.SPA.pkg
      File is in use, will not delete.
    cat9k-sipspa.16.06.02.SPA.pkg
      File is in use, will not delete.
    cat9k-srdriver.16.06.02.SPA.pkg
      File is in use, will not delete.
    cat9k-webui.16.06.02.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

The following files will be deleted:
[R0]:
/flash/cat9k-cc_srdriver.16.06.02.SPA.pkg
/flash/cat9k-espbase.16.06.02.SPA.pkg
/flash/cat9k-guestshell.16.06.02.SPA.pkg
/flash/cat9k-rpbase.16.06.02.SPA.pkg
/flash/cat9k-rpboot.16.06.02.SPA.pkg
/flash/cat9k-sipbase.16.06.02.SPA.pkg
/flash/cat9k-sipspa.16.06.02.SPA.pkg
/flash/cat9k-srdriver.16.06.02.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.16.06.02.SSA.bin
/flash/packages.conf.00-

Do you want to remove the above files? [y/n]y
[R0]:
Deleting file flash:cat9k-cc_srdriver.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.06.02.SPA.pkg ... done.
```

```
Deleting file flash:cat9k-rpbase.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.02.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.B16.06.02.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#
```

Copy New Image to Flash

Step 2 Copy the target Cisco IOS XE Everest 16.6.1 image to flash: (you can skip this step if you want to use the image from your TFTP server).

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.06.01.SPA.bin flash:
Destination filename [cat9k_iosxe.16.06.01.SPA.bin]?

Accessing tftp://10.8.0.6//cat9k_iosxe.16.06.01.SPA.bin...
Loading /cat9k_iosxe.16.06.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 508584771 bytes]

508584771 bytes copied in 101.005 secs (5035244 bytes/sec)
```

Step 3 Use the **dir flash** 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  Jul 26 2017 13:35:16 -07:00  cat9k_iosxe.16.06.01.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Downgrade Software Image

Step 4 Use the **install add file activate commit** command, to downgrade your switch. 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.16.06.01.SPA.bin activate commit

install_add_activate_commit: START Fri Jun  9 22:49:41 UTC 2017

*Jun  9 22:49:42.772: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jun  9 22:49:42
install_engine.sh: %INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.06.01.SPA.bin
install_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.06.01.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.16.06.01.SPA.pkg
/flash/cat9k-srdriver.16.06.01.SPA.pkg
/flash/cat9k-sipspa.16.06.01.SPA.pkg
/flash/cat9k-sipbase.16.06.01.SPA.pkg
/flash/cat9k-rpboot.16.06.01.SPA.pkg
/flash/cat9k-rpbase.16.06.01.SPA.pkg
/flash/cat9k-espbase.16.06.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.06.01.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.16.06.01.SPA.pkg
/flash/cat9k-srdriver.16.06.01.SPA.pkg
/flash/cat9k-sipspa.16.06.01.SPA.pkg
/flash/cat9k-sipbase.16.06.01.SPA.pkg
/flash/cat9k-rpboot.16.06.01.SPA.pkg
```

```
/flash/cat9k-rpbase.16.06.01.SPA.pkg
/flash/cat9k-guestshell.16.06.01.SPA.pkg
/flash/cat9k-espbase.16.06.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.06.01.SPA.pkg
Fri Jun  9 22:53:58 UTC 2017
Switch#
```

To downgrade your switch, you can also use the **install rollback to committed** command.

Note 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 Thu Nov  2 14:24:56 UTC 2017

This operation requires a reload of the system. Do you want to proceed? [y/n]
                                                                                *Nov  2
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.16.06.02.SPA.pkg
    Current    :  rp 1  0 rp_boot       cat9k-rpboot.16.06.02.SPA.pkg
    Replacement:  rp 0  0 rp_boot       cat9k-rpboot.16.06.01.SPA.pkg
    Replacement:  rp 1  0 rp_boot       cat9k-rpboot.16.06.01.SPA.pkg
    Current    :  cc 0  0 cc_srdriver   cat9k-cc_srdriver.16.06.02.SPA.pkg
    Current    :  cc 0  0 cc            cat9k-sipbase.16.06.02.SPA.pkg
    Current    :  cc 0  0 cc_spa        cat9k-sipspa.16.06.02.SPA.pkg
    Current    :  cc 1  0 cc_srdriver   cat9k-cc_srdriver.16.06.02.SPA.pkg
    Current    :  cc 1  0 cc            cat9k-sipbase.16.06.02.SPA.pkg
    Current    :  cc 1  0 cc_spa        cat9k-sipspa.16.06.02.SPA.pkg
    Current    :  cc 10 0 cc            cat9k-sipbase.16.06.02.SPA.pkg
    Current    :  cc 10 0 cc_spa        cat9k-sipspa.16.06.02.SPA.pkg
    Current    :  cc 10 0 cc_srdriver   cat9k-cc_srdriver.16.06.02.SPA.pkg
    Current    :  cc 2  0 cc_srdriver   cat9k-cc_srdriver.16.06.02.SPA.pkg
    Current    :  cc 2  0 cc            cat9k-sipbase.16.06.02.SPA.pkg
    Current    :  cc 2  0 cc_spa        cat9k-sipspa.16.06.02.SPA.pkg
    Current    :  cc 3  0 cc_srdriver   cat9k-cc_srdriver.16.06.02.SPA.pkg
    Current    :  cc 3  0 cc            cat9k-sipbase.16.06.02.SPA.pkg
    Current    :  cc 3  0 cc_spa        cat9k-sipspa.16.06.02.SPA.pkg
    Current    :  cc 4  0 cc_srdriver   cat9k-cc_srdriver.16.06.02.SPA.pkg
    Current    :  cc 4  0 cc            cat9k-sipbase.16.06.02.SPA.pkg
    Current    :  cc 4  0 cc_spa        cat9k-sipspa.16.06.02.SPA.pkg
    Current    :  cc 5  0 cc_srdriver   cat9k-cc_srdriver.16.06.02.SPA.pkg
    Current    :  cc 5  0 cc            cat9k-sipbase.16.06.02.SPA.pkg
    Current    :  cc 5  0 cc_spa        cat9k-sipspa.16.06.02.SPA.pkg
    Current    :  cc 6  0 cc_srdriver   cat9k-cc_srdriver.16.06.02.SPA.pkg
    Current    :  cc 6  0 cc            cat9k-sipbase.16.06.02.SPA.pkg
    Current    :  cc 6  0 cc_spa        cat9k-sipspa.16.06.02.SPA.pkg
    Current    :  cc 7  0 cc_srdriver   cat9k-cc_srdriver.16.06.02.SPA.pkg
    Current    :  cc 7  0 cc            cat9k-sipbase.16.06.02.SPA.pkg
    Current    :  cc 7  0 cc_spa        cat9k-sipspa.16.06.02.SPA.pkg
    Current    :  cc 8  0 cc_srdriver   cat9k-cc_srdriver.16.06.02.SPA.pkg
    Current    :  cc 8  0 cc            cat9k-sipbase.16.06.02.SPA.pkg
    Current    :  cc 8  0 cc_spa        cat9k-sipspa.16.06.02.SPA.pkg
```

```
Current    :  cc 9   0 cc_srdriver   cat9k-cc_srdriver.16.06.02.SPA.pkg
Current    :  cc 9   0 cc            cat9k-sipbase.16.06.02.SPA.pkg
Current    :  cc 9   0 cc_spa        cat9k-sipspa.16.06.02.SPA.pkg
Current    :  fp 0   0 fp            cat9k-espbase.16.06.02.SPA.pkg
Current    :  fp 1   0 fp            cat9k-espbase.16.06.02.SPA.pkg
Current    :  rp 0   0 guestshell    cat9k-guestshell.16.06.02.SPA.pkg
Current    :  rp 0   0 rp_base       cat9k-rpbase.16.06.02.SPA.pkg
Current    :  rp 0   0 rp_daemons    cat9k-rpbase.16.06.02.SPA.pkg
Current    :  rp 0   0 rp_iosd       cat9k-rpbase.16.06.02.SPA.pkg
Current    :  rp 0   0 rp_security   cat9k-rpbase.16.06.02.SPA.pkg
Current    :  rp 0   0 rp_webui      cat9k-webui.16.06.02.SPA.pkg
Current    :  rp 0   0 rp_wlc        cat9k-wlc.16.06.02.SPA.pkg
Current    :  rp 0   0 srdriver      cat9k-srdriver.16.06.02.SPA.pkg
Current    :  rp 1   0 guestshell    cat9k-guestshell.16.06.02.SPA.pkg
Current    :  rp 1   0 rp_base       cat9k-rpbase.16.06.02.SPA.pkg
Current    :  rp 1   0 rp_daemons    cat9k-rpbase.16.06.02.SPA.pkg
Current    :  rp 1   0 rp_iosd       cat9k-rpbase.16.06.02.SPA.pkg
Current    :  rp 1   0 rp_security   cat9k-rpbase.16.06.02.SPA.pkg
Current    :  rp 1   0 rp_webui      cat9k-webui.16.06.02.SPA.pkg
Current    :  rp 1   0 rp_wlc        cat9k-wlc.16.06.02.SPA.pkg
Current    :  rp 1   0 srdriver      cat9k-srdriver.16.06.02.SPA.pkg
Replacement:  cc 0   0 cc_srdriver   cat9k-cc_srdriver.16.06.01.SPA.pkg
Replacement:  cc 0   0 cc            cat9k-sipbase.16.06.01.SPA.pkg
Replacement:  cc 0   0 cc_spa        cat9k-sipspa.16.06.01.SPA.pkg
Replacement:  cc 1   0 cc_srdriver   cat9k-cc_srdriver.16.06.01.SPA.pkg
Replacement:  cc 1   0 cc            cat9k-sipbase.16.06.01.SPA.pkg
Replacement:  cc 1   0 cc_spa        cat9k-sipspa.16.06.01.SPA.pkg
Replacement:  cc 10  0 cc            cat9k-sipbase.16.06.01.SPA.pkg
Replacement:  cc 10  0 cc_spa        cat9k-sipspa.16.06.01.SPA.pkg
Replacement:  cc 10  0 cc_srdriver   cat9k-cc_srdriver.16.06.01.SPA.pkg
Replacement:  cc 2   0 cc_srdriver   cat9k-cc_srdriver.16.06.01.SPA.pkg
Replacement:  cc 2   0 cc            cat9k-sipbase.16.06.01.SPA.pkg
Replacement:  cc 2   0 cc_spa        cat9k-sipspa.16.06.01.SPA.pkg
Replacement:  cc 3   0 cc_srdriver   cat9k-cc_srdriver.16.06.01.SPA.pkg
Replacement:  cc 3   0 cc            cat9k-sipbase.16.06.01.SPA.pkg
Replacement:  cc 3   0 cc_spa        cat9k-sipspa.16.06.01.SPA.pkg
Replacement:  cc 4   0 cc_srdriver   cat9k-cc_srdriver.16.06.01.SPA.pkg
Replacement:  cc 4   0 cc            cat9k-sipbase.16.06.01.SPA.pkg
Replacement:  cc 4   0 cc_spa        cat9k-sipspa.16.06.01.SPA.pkg
Replacement:  cc 5   0 cc_srdriver   cat9k-cc_srdriver.16.06.01.SPA.pkg
Replacement:  cc 5   0 cc            cat9k-sipbase.16.06.01.SPA.pkg
Replacement:  cc 5   0 cc_spa        cat9k-sipspa.16.06.01.SPA.pkg
Replacement:  cc 6   0 cc_srdriver   cat9k-cc_srdriver.16.06.01.SPA.pkg
Replacement:  cc 6   0 cc            cat9k-sipbase.16.06.01.SPA.pkg
Replacement:  cc 6   0 cc_spa        cat9k-sipspa.16.06.01.SPA.pkg
Replacement:  cc 7   0 cc_srdriver   cat9k-cc_srdriver.16.06.01.SPA.pkg
Replacement:  cc 7   0 cc            cat9k-sipbase.16.06.01.SPA.pkg
Replacement:  cc 7   0 cc_spa        cat9k-sipspa.16.06.01.SPA.pkg
Replacement:  cc 8   0 cc_srdriver   cat9k-cc_srdriver.16.06.01.SPA.pkg
Replacement:  cc 8   0 cc            cat9k-sipbase.16.06.01.SPA.pkg
Replacement:  cc 8   0 cc_spa        cat9k-sipspa.16.06.01.SPA.pkg
Replacement:  cc 9   0 cc_srdriver   cat9k-cc_srdriver.16.06.01.SPA.pkg
Replacement:  cc 9   0 cc            cat9k-sipbase.16.06.01.SPA.pkg
Replacement:  cc 9   0 cc_spa        cat9k-sipspa.16.06.01.SPA.pkg
Replacement:  fp 0   0 fp            cat9k-espbase.16.06.01.SPA.pkg
Replacement:  fp 1   0 fp            cat9k-espbase.16.06.01.SPA.pkg
Replacement:  rp 0   0 guestshell    cat9k-guestshell.16.06.01.SPA.pkg
Replacement:  rp 0   0 rp_base       cat9k-rpbase.16.06.01.SPA.pkg
Replacement:  rp 0   0 rp_daemons    cat9k-rpbase.16.06.01.SPA.pkg
Replacement:  rp 0   0 rp_iosd       cat9k-rpbase.16.06.01.SPA.pkg
Replacement:  rp 0   0 rp_security   cat9k-rpbase.16.06.01.SPA.pkg
Replacement:  rp 0   0 rp_webui      cat9k-webui.16.06.01.SPA.pkg
Replacement:  rp 0   0 srdriver      cat9k-srdriver.16.06.01.SPA.pkg
Replacement:  rp 1   0 guestshell    cat9k-guestshell.16.06.01.SPA.pkg
```

```
    Replacement:  rp 1  0 rp_base       cat9k-rpbase.16.06.01.SPA.pkg
    Replacement:  rp 1  0 rp_daemons    cat9k-rpbase.16.06.01.SPA.pkg
    Replacement:  rp 1  0 rp_iosd       cat9k-rpbase.16.06.01.SPA.pkg
    Replacement:  rp 1  0 rp_security   cat9k-rpbase.16.06.01.SPA.pkg
    Replacement:  rp 1  0 rp_webui      cat9k-webui.16.06.01.SPA.pkg
    Replacement:  rp 1  0 srdriver      cat9k-srdriver.16.06.01.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  Thu Nov  2 14:26:35 UTC 2017

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

Initializing Hardware...

System Bootstrap, Version 16.6.2r[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
16.6.1, 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 5 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
```

Step 6 When the new image boots up, you can verify the version of the new image, by checking **show version**

Note In the output, note that the boot loader is not automatically downgraded. It will remain updated.

```
Switch# show version

isco IOS XE Software, Version 16.06.01
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.6.1, 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.

ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 16.6.2r[FC2], RELEASE SOFTWARE (P)

Switch uptime is 1 minute
Uptime for this control processor is 2 minutes
System returned to ROM by reload
System image file is "bootflash:packages.conf"
Last reload reason: LocalSoft

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.

Technology Package License Information:

------------------------------------------------------------------
Technology-package                  Technology-package
Current             Type            Next reboot
------------------------------------------------------------------
network-advantage   Permanent       network-advantage

cisco C9410R (X86) processor (revision V00) with 868521K/6147K bytes of memory.
Processor board ID FXS2118Q1GM
1 Virtual Ethernet interface
312 Gigabit Ethernet interfaces
24 Ten 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:.

Configuration register is 0x2
Switch#
```

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 9000 Series Switches fall under the 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—Require a Network Essentials or 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 http://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—for a license level, preinstalled on the device, and for a 90-day trial period only.

Ordering with Smart Accounts

We recommend that you use Smart Accounts to order devices as well as licenses. Smart Accounts enable you to manage all of your software licenses for switches, routers, firewalls, access-points or tools from one centralized website. To create Smart Accounts, use the Cisco Smart Software Manager (Cisco SSM).

Note This is especially relevant to the term licenses that you order, because information about the expiry of term licenses is available only through the Cisco SSM website.

For information more information about Cisco SSM, see:
http://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html

The possible deployment modes are:

- Right-to-use (RTU) licensing mode—Supported on Cisco Catalyst 9000 Series Switches. See The RTU Licensing Mode, page 32.

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**] [**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 8 Permitted Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No
Network Advantage	Yes[1]	Yes

1. 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 the feature 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 S*ystem Management* > *Configuring Right-To-Use Licenses* chapter of the software configuration guide for your software release:
https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/products-installation-and-configuration-guides-list.html.

Scaling Guidelines

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

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739055.html

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.html

Limitations and Restrictions

- Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
- Control Plane Policing (CoPP)—Starting with Cisco IOS XE Everest 16.6.4, 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 s**how policy-map control-plane** commands in privileged EXEC mode instead.
- Flexible NetFlow (FNF) 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 the same type (ipv4, ipv6 or datalink) on the same interface, in the same direction.
- 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.
- QoS restrictions:
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.

  - For QoS policies, only SVIs 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 in IOS XE Everest 16.6.2. The associated route processor redundancy (RPR) feature is currently not supported.
  Use the **show redundancy** and **show platform software iomd redundancy** commands to ensure that both SSO formed and IOMD is ready before doing any switchover.
- Secure Shell (SSH)
  - Use SSH Version 2. SSH Version 1 is not supported.
  - When the device is running SCP (Secure Copy Protocol) 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.
- Smart Install— The commands are visible on the CLI in Cisco IOS XE Everest 16.6.1, but the feature is not supported. Enter the **no vstack** command in global configuration mode and disable the feature. Starting from Cisco IOS XE Everest 16.6.2, the **vstack** command is not available on the CLI.
- Uplink Symmetry—When a redundant supervisor is inserted, it is recommended to have symmetric uplinks, so that packet loss during a switchover is minimal.
  - Uplinks are said to be in symmetry when the same interface in both supervisors have the same type of transceiver module. A TenGigabitEthernet interface with no transceiver operates at default 10G mode, and if the matching interface of the other supervisor has a 10G transceiver, then they are in symmetry. Symmetry gives 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.

Caveats

Caveats describe unexpected behavior in Cisco IOS 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 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 Everest 16.6.x

The following are the open caveats in this release:

Identifier	Headline
CSCve21940	C9400 Cannot ping phone/data client with IPSG
CSCvh97897	Copper GE T SFP not able detect by system SW after optic OIR
CSCvj82886	FNF export not working after second switchover when ETA+FNF is configured
CSCvk60809	Wrong Time-Stamp is saved in pcap.
CSCvn87418	cmanfp do not report serdes sync error in case of Doppler D local fault.
CSCvp10506	C9400 : %IOSXE-2-PLATFORM: Switch 1 R0/0: kernel: EXT2-fs (sda1): error:
CSCvq72713	Cat3k/Cat9k can't forwarding traffic follow the rule of EIGRP unequal cost load-balancing
CSCvq93745	C9400 - Unable to edit FNF commands after pull out a LC

Resolved Caveats in Cisco IOS XE Everest 16.6.10

Identifier	Description
CSCvt53563	Cisco IOS XE Software NETCONF and RESTCONF Authentication Bypass Vulnerability
CSCvw25564	Cisco IOS and IOS XE Software IKEv2 AutoReconnect Feature Denial of Service Vulnerability
CSCvw46194	IOS and IOS XE Software UDLD Denial of Service Vulnerability
CSCvx41294	High CPU usage caused by "TCP Timer" process
CSCvx66699	Cisco IOS and IOS XE Software TrustSec CLI Parser Denial of Service Vulnerability

Resolved Caveats in Cisco IOS XE Everest 16.6.9

Identifier	Description
CSCvf75522	Traffic incorrectly matches an ACL-based class-map that contains 'range' operations
CSCvo67790	Switch crash seen when unconfig/defaulting macsec session over a range of interfaces
CSCvt22293	C9400: %PMAN-0-PROCFAILCRIT: R0/0: pvp: A critical process command has failed
CSCvt30243	Connectivity issue after moving client from dot1x enable port to non dot1x port
CSCvt74856	C9407R Operating Redundancy mode shown as SSO after standby SUP fullly booting up.
CSCvu30597	Cisco IOS XE Software Ethernet Frame Denial of Service Vulnerability
CSCvu95137	SNMP monitoring tool time out for ciscoEntitySensorMIB 1.3.6.1.4.1.9.9.91.1.1.1.1
CSCvv48305	Route not fully programmed in the hardware for MACSec enabled end-point

Resolved Caveats in Cisco IOS XE Everest 16.6.8

Identifier	Description
CSCvm40582	Crash when entering username with aaa common-criteria policy password
CSCvo36359	C9400: Enable TestUnusedPortLoopback.
CSCvp73666	DNA - LAN Automation doesn't configure link between Peer Device and PnP Agent due CDP limitation
CSCvp81958	Cat9x00 hitting "No connections to Shell Manager available for processing the command"
CSCvq39840	CiscoFlashFile - Get-Next request takes longer time for last file on directory.
CSCvr03905	Memory Leak on FED due to IPv6 Source Guard
CSCvr20522	Cat3k/9k BOOTREPLY dropped when DHCP snooping is enabled
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)
CSCvr98506	Shut down interfaces range of TenGig Ports on the Active Sup randomly causing flaps 40gig ports.

Resolved Caveats in Cisco IOS XE Everest 16.6.7

Identifier	Description
CSCvf42299	User defined System MTU is not taking effect on PO and SVI
CSCvj16691	port LED may turn to amber
CSCvn81334	Default ACL being enforced even when dACL is applied after Reload
CSCvo65974	QinQ tunnels causing L2 loop in specific topology.

Identifier	Description
CSCvo71264	Gateway routes DHCP offer incorrectly after DHCP snooping
CSCvo83305	MAC Access List Blocks Unintended Traffic
CSCvo85183	Uplinkfast take time when recovery from link failure
CSCvo85422	Directly connected IPv4/IPv6 hosts not programmed in HW - %FMFP-3-OBJ_DWNLD_TO_DP_FAILED
CSCvo94058	URPF packet drop despite "rx allow-default" option
CSCvp00026	No audio during first few seconds of voice call between 2 Fabric Edge
CSCvp15389	Port security configuration on interface causing connectivity issue
CSCvp26792	Control plane impacted when > 1Gbps multicast passes through and no entry in IGMP snooping
CSCvp30239	Memory leak when there are constant changes in REP ring
CSCvp33294	Asic 0 Core 0 buffer stuck, rwePbcStall seen
CSCvp40743	Switch crashing after running 'test platform soft fed active xcvr lpn <> <> dump <> <>' command
CSCvp43131	Mgmt port "speed 1000" and "negotiation auto" in show run
CSCvp54581	C9400-LC-48U fails POST after Hot Swapping with C9400-LC-48UX/C9400-LC-24XS
CSCvp54779	[SDA] 1st ARP Reply is dropped at remote Fabric Edge
CSCvp55337	Uplink Port Channel Link Flap After Active SUP removal
CSCvp69629	Authentication sessions does not come up on configuring dot1x when there is active client traffic.
CSCvp75221	Modules shows faulty status when specific MAC ACL is applied on interfaces
CSCvp89755	VPN label is wrongly derived as explicit-null in Cat9k for L3 VPN traffic
CSCvp90279	ADV and REP DHCPv6 packets are sent to SISF when source udp port is not 547
CSCvq17688	Packets could loop between supervisor and linecard.
CSCvq22011	ARP replies are dropped when IPDT gleans from ARP
CSCvq30316	[SDA] 1st ARP fix for CSCvp00026 is eventually failing after longevity
CSCvq30460	SYS-2-BADSHARE: Bad refcount in datagram_done - messages seen during system churn
CSCvq40137	Mac address not being learnt when "auth port-control auto" command is present
CSCvq44397	ospf down upon switchover with aggressive timers "hello-interval 1" and "dead-interval 4"
CSCvq91675	The active and the standby Sup crashes due to ccmc crash when upgraded.

Resolved Caveats in Cisco IOS XE Everest 16.6.6

Identifier	Description
CSCvn08296	DNA Center 1.2.5 - SDA Border as RP incorrectly resolving RPF next-hop as LISP interface
CSCvo32446	High CPU Due To Looped Packet and/or Unicast DHCP ACK Dropped
CSCuw36080	SNMP with Extended ACL
CSCvg73991	PBR adjacency not getting updated correctly after shut/no shut on interface
CSCvm07353	Router may crash when a SSH session is closed after configure TACACS
CSCvm48084	Remark in DACL causes Authorization failure
CSCvm55520	C9407R-C9400-PWR-3200AC Power Supply goes into faulty state randomly ("n.a.")
CSCvm82912	C9400/16.6.4- standby sup port shows green LED even when port is err-disabled due to POST fail
CSCvm89086	SPAN destination interface not dropping ingress traffic
CSCvn01822	cmnMacMoveNotification is generated when a MAC address is moved between same Port-channel interface
CSCvn23706	no mac address-table notification mac-move can't be saved after reload device
CSCvn31477	Layer 2 SSM Multicast traffic hitting the CPU when SVI is configured with PIM Spare Mode
CSCvn46517	some sgacl were not installed after update a Cell in ISE
CSCvn56579	MQIPC memory corruption resulting dot1x/MAB not working for wired clients
CSCvn72973	Device is getting crashed on the "cts role-based enforcement"
CSCvn74807	Cisco TrustSec crash while processing CoA update
CSCvn79221	MAC ADDRESS LEARNING FAILURE ON PORT CONFIGURED WITH PORT-SECURITY
CSCvo15594	MATM programming issue for remote client
CSCvo42353	SDA; Cat3K,Cat9K:-External border creating incorrect CEF/map-cache entry due to multicast

Resolved Caveats in Cisco IOS XE Everest 16.6.5

Identifier	Description
CSCvh79433	C9400: "kernel: ICMPv6: NA: someone advertises our address" seen when neighbor bootup
CSCvh85885	IPv6 stale entries not expiring
CSCvh89452	[C9400]FCV:On "reload/redundancy reload shelf" CLI - standby comes as active (interim) at-times
CSCvi81569	FNF is not exporting after reload when ETA + FNF enabled on interface
CSCvi96965	Radius Automate Tester probe on feature is not working as expected.

Identifier	Description
CSCvj79694	sgt-map gets cleared for some of the end points for unknown reason
CSCvj92201	16.6.4:Device-tracking does not consistenly show DH4 for DHCP clients
CSCvk06087	mGig ports on C9400 - Link down with forced speed 100/full duplex when connect to half duplex device
CSCvk12880	Cat9400 Fails USGv6 Multicast Routing Tests
CSCvk20003	Polaris: Host limit of 32 for session monitoring sessions
CSCvk30813	MAB fails to start negotiation after device moves to another layer 2 adjacent switch
CSCvk32866	SISF probing behavior should be changed from broadcast to unicast
CSCvk34927	DHCP snooping table not updated from DHCP snooping DB file upon reload.
CSCvk39041	SDA: IP phone latency in fabric is close to 4 sec's
CSCvk60752	DHCP offer with Option 82 but no Remote ID suboption dropped by CAT9K relay agent
CSCvk63089	show logging onboard switch active uptime detail shows 133 years as uptime
CSCvm00765	BFD crash on imitating traffic loss
CSCvm33622	WCCP redirection to proxy server breaks in certain scenarios.
CSCvm35904	16.6.3: Access Tunnel Create Interface code is considered to be update request in FMAN_FP
CSCvm36333	MAC address programming issue
CSCvm39894	False authorizations and authentications even without radius server for dot1x/mab
CSCvm43071	[IBNS 2.0] aaa-available event is not being triggered when using authentication/authorization list
CSCvm46814	session management process smd crash at cts_sga due to TDL memory depletion.
CSCvm47139	Catalyst 3850/9300 Switches not providing PoE+ power for APs
CSCvm60720	Broadcast Gratuitous ARP changed to unicast by switch leading to DHCP decline from client
CSCvm62274	Multicast traffic is software switched when switch is provisioned as Edge in Fabric - SDA Deployment
CSCvm63651	Memory leak due to authentication mac-move permit
CSCvm68064	Cat 9400: MAC address entries not cleared out after aging
CSCvm75378	Cat9x00: IPv6 SPAN filter still applied in hardware when removing entire monitor session
CSCvm86135	SMD crash after removing access-session attributes filter-list
CSCvm89005	Packets looped internally during VXLAN decap in SD-Access environment
CSCvm95352	uRPF TCAM Resources exhausted even without uRPF configured on the switch
CSCvm97660	C9300 reflects back traffic on the same interface
CSCvn08672	DHCP packets cause unknown protocol drops on 16.6.x

Identifier	Description
CSCvn36398	WCCP Access-list might not be removed from interface after a WCCP loss of service
CSCvn46171	Rapid Memory Leak in "FED Main Event" Process due to Modifying Adjacencys

Resolved Caveats in Cisco IOS XE Everest 16.6.4a

Identifier	Description
CSCvj83551	SISF crash in IPV6 neighbor discovery packets
CSCvm35904	16.6.3: Access Tunnel Create Interface code is considered to be update request in FMAN_FP
CSCvm09611	C9x00 crashed with multicast memory corruption.
CSCvk60752	DHCP offer with Option 82 but no Remote ID suboption dropped by CAT9K relay agent
CSCvk32774	ACE entry with *established or range * in ACL drops TCP/UDP packets.
CSCvk31115	Device-sensor doesn't send data off initial boot
CSCvj86644	SDA: DHCP does not remove option 82 when sending packets to end-hosts
CSCvk39041	SDA: IP phone latency in fabric is close to 4 sec's
CSCvk02589	Connectivity is lost every four hours when ipv4 and ipv6 dual stack is configured.
CSCvj94357	Catalyst 9400 Line card may go to 'Faulty' status after reload.
CSCvk27755	9410:Duplicate client LE index assigned to the client over slot 9 & slot 10 (CSCvi09442)
CSCvk32563	Catalyst 9400 cmand memory leak
CSCvm68064	Cat 9400: MAC address entries not cleared out after aging
CSCvj33865	Clearing mac address table should not delete entries created by control plane/remote entries
CSCvk07070	Observing bmalloc smd leaks at OBJ_WEBAUTH_LOGOUT_URL with webauth
CSCvk16813	DHCP client traffic dropped with DHCP snooping and port-channel or cross stack uplinks.
CSCvk46664	DNA Center SWIM Upgrade fails and unable to upgrade manually
CSCvk50734	Device Tracking - Memory leak observed with IPv6 NS/NA Packets .
CSCvk53444	Packets with Fragment Offset not forwarded with DHCP Snooping Enabled in 16.6.4
CSCvm01064	PE stops VPLS traffic forwarding after xconnect flap
CSCvm09121	Evaluation of IOS-XE for CVE-2018-5391 (FragmentSmack)

Resolved Caveats in Cisco IOS XE Everest 16.6.4

The following are the resolved caveats in Cisco IOS XE Everest 16.6.4.

Identifier	Description
CSCvh87176	switch console may freeze on running "sh platform software fed active ip multicast groups"
CSCvh50172	MPLS L3VPN traffic is dropped due to Wrong bgp vpn label (exp null)
CSCvi83373	Repetitive logs show up 47K times in fed tracelogs
CSCvj52681	dynamic vlan assignment causes all sisf entires under the port to be deleted
CSCvi91714	IPv6 address not assigned or delayed when RA Guard is enabled
CSCvi76084	Device-tracking entry stuck in TENTATIVE for certain Mac Pro hosts configured with static IP
CSCvi38916	Persistent Telnet and SSH crashes when configured in 16.6.2
CSCvi26398	"%LISP-4-LOCAL_EID_RLOC_INCONSISTENCY" should be supporessed in SDA context
CSCvi20882	Netconf IP-SLA udp-jitter case missing leaf codec
CSCvi11970	Abnormal output for show pnp tech-support
CSCvh85772	Switch not responding to ARP request for GW Anycast IP
CSCvh79942	Chunk corruption crash related to PNP or Guestshell
CSCvh21909	LISP: Overlapping prefix causes "probe-down" for map-cache entry
CSCvh09334	SDA-IPV6::SISF traceback @ar_relay_create_entry - L2 Binding tbl entry insertion failed
CSCvg45950	packet drop seen intermittently if 40G traffic sent via cts interface
CSCvf36816	cat9400-16.6.1 bootup error/warning messages - no functional impact
CSCvb69966	Memory leak under LLDP Protocol process
CSCvg53159	%SNMP-3-RESPONSE_DELAYED: processing GetNext of cafSessionEntry.2 seen on catalyst switch.
CSCvi95676	TAN number in IDPROM shouldn't be hard coded
CSCvi93137	Voice domain not forwarding for certain clients
CSCvi77574	16.6.3 Packets mapped to wrong DGTid
CSCvi39202	DHCP fails when DHCP snooping trust is enabled on uplink etherchannel
CSCvh11396	Switchport Security Command triggering Bulk Sync Failure
CSCvg71118	Dot1x configuration on AP Trunk Ports causes unreachability
CSCvg56874	9400: System LED became RED after Active SUP OIR
CSCvh71930	show chassis power-supply detail report "PEC error"
CSCvh84345	IOS CLI "show platform software fed switch active punt cause summary" may display negative counts
CSCvi34262	Process flash_util,Hman crashes in the absence of /dev/mtdblock with multiple reload test
CSCvi38191	Memory leak in lman process due to "ld_license_ext.dat" build-up.
CSCvj38312	Power priority non unique slots causing IOS crash
CSCvg41950	Cisco IOS XE Software Diagnostic Shell Path Traversal Vulnerability

Identifier	Description
CSCvh71539	Command "show aaa servers" reloads the switch
CSCvj49476	Telnet Sessions Hang/Become unavailable at execution of "show run"

Resolved Caveats in Cisco IOS XE Everest 16.6.3

The following are the resolved caveats in Cisco IOS XE Everest 16.6.3:

Identifier	Headline
CSCvg00911	PVLAN client entry moves to STALE state when for Active client with DHCP Snooping.
CSCvg08401	Catalyst 9400 IOMD crashed on new active@iomd_timer_handler during 1st SWO (interim).
CSCvg09754	IPv6 PBR not working after an SSO.
CSCvg24428	CISP client table is empty after link connected and clients authz.
CSCvg26068	16.6.2 LDP traffic do not resume after SSO with multiple core facing SVI.
CSCvg38873	Catalyst 9400-LC-24XS: Some transceivers become unsupported when doing SFP OIR after Active Sup OIR.
CSCvf39207	L2pt tunnel moving to err-disable state when point-to-point lacp links are shut and no shut.
CSCvg39909	Catalyst 9400 switch will not increment output drop counters.
CSCvg60597	Catalyst 9400-SUP-1: On uplinks, speed config of 10m/100m on GLC-T results in traffic failure.
CSCvg81945	Catalyst 9400: Standby SUP might crash during bootup on 10 slot chassis with 8 LC.
CSCvg55327	C9400 10 slot chassis may fail to boot with 4 or more than 4 linecards when slot 10 is empty.
CSCvg78413	Catalyst 9400: "sh idprom" for New ECI number.
CSCvh31431	Memory leak in linux_iosd-image on 16.6 releases.
CSCvh52882	Memory Leak due to nbar config.
CSCvh69402	Dot1x specific configuration applied but not working on the interface.
CSCvh81152	Local SVI IP is registered as dynamic-eid.
CSCvg81945	Cat9400 Standby SUP takes longer to reach SSO at when 10 slot chassis has 8 LC and 8 power supplies.
CSCvh06383	16.6.x: Intermittent traffic loss for MAB devices after successful intial authentication.
CSCvf51884	QoS ingress cos classification failed on trust cos dot1q-tunnel port.
CSCvg57547	[c94k 40gb] No dataplane traffic on 40gb ports due to issues with QSFP.
CSCvg56727	crashes with 'server-key' command using key of 128 characters or more.
CSCve32330	%UTIL-6-RANDOM: A pseudo-random number was generated twice in succession.
CSCvg22515	After upgrade of IOS, SSH passwords longer than 25 characters do not work.

CSCvg60288	Device IP address AV pair replaced with 192.168.1.5.
CSCvh32416	Evaluation of all for CPU Side-Channel Information Disclosure Vulnerability.
CSCvh55578	To add recovery mechanism for glean entry.
CSCvf84349	Router crash on polling cEigrpPeerEntry.

Resolved Caveats in Cisco IOS XE Everest 16.6.2

The following are the resolved caveats in Cisco IOS XE Everest 16.6.2.

Identifier	Description
CSCve20614	Snmpset is failing for Dot3PauseExtAdminMode object on x86 image.
CSCve78881	Catalyst 9400: OIDs have to be unique for 40G QSFPs under 'show inventory oid' output.
CSCve95723	For few copper SFP, the **show inventory** command does not show PID data.
CSCvf06005	CRC error packets are observed on peer: (Local port: with 1G-->100M speed change).
CSCvf75518	Controller port error interface.

Troubleshooting

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

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

Choose **Product Support > Switches**. Then choose your product and click **Troubleshoot and Alerts** to find information for the problem that you are experiencing.

Related Documentation

- Cisco Catalyst 9400 Series Switches documentation at this URL:

  http://www.cisco.com/go/c9400
- Cisco IOS XE 16 documentation at this URL:

  http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html
- Cisco transceiver module documentation, including compatibility information at this URL:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html
- Cisco Validated Designs documents at this URL:

  http://www.cisco.com/go/designzone

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation*, which lists all new and revised Cisco Technical documentation, as an RSS feed and deliver content directly to your desktop using a read application. The RSS feeds are a free service.

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: www.cisco.com/go/trademarks. 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)

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.

© 2019 Cisco Systems, Inc. All rights reserved.