Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Fuji 16.9.x

First Published: 2018-07-18

Last Modified: 2021-09-01

Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Fuji 16.9.x

Introduction

Cisco Catalyst 9300 Series Switches are Cisco's lead stackable access platform for the next-generation enterprise and has been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

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

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

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

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

Do provide feedback about your experience with the Content Hub.

Whats New in Cisco IOS XE Fuji 16.9.8

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 40.

Whats New in Cisco IOS XE Fuji 16.9.7

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 40.

Software Features in Cisco IOS XE Fuji 16.9.7

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

Whats New in Cisco IOS XE Fuji 16.9.6

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 40.

Whats New in Cisco IOS XE Fuji 16.9.5

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 40.

Whats New in Cisco IOS XE Fuji 16.9.4

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 40.

Whats New in Cisco IOS XE Fuji 16.9.3

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 40.

Whats New in Cisco IOS XE Fuji 16.9.2

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 40.

Whats New in Cisco IOS XE Fuji 16.9.1

Hardware Features in Cisco IOS XE Fuji 16.9.1

Feature Name	Description and Documentation Link
Cisco 40GBASE QSFP Module (4x10G mode qualification)	• Supported transceiver module number—QSFP-40G-CSR4 • Compatible network modules—C9500-NM-2Q uplinks For information about the module, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix.
Cisco 25GBASE SFP28 Modules	Supported transceiver module numbers— • SFP-25G-SR-S • SFP-10/25G-CSR-S (supports 10G and 25G speeds with network module C9300-NM-2Y) • SFP-25G-AOC1M, SFP-25G-AOC2M, SFP-25G-AOC3M, SFP-25G-AOC4M, SFP-25G-AOC5M, SFP-25G-AOC7M, SFP-25G-AOC10M For information about the module, see the Cisco 25GBASE SFP28 Modules Data Sheet. For information about compatibility with a device, see the Cisco 25-Gigabit Ethernet Transceiver Modules Compatibility Matrix.
Cisco 40GBASE QSFP Module— QSFP-4X10G-AOC	Supported transceiver module numbers—QSFP-4X10G-AOC1M, QSFP-4X10G-AOC2M, QSFP-4X10G-AOC3M, QSFP-4X10G-AOC5M, QSFP-4X10G-AOC7M, QSFP-4X10G-AOC7M. For information about the module, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix.
USB 3.0 Solid State Drive (SSD) Part number: SSD-120G	A pluggable drive that provides an extra 120GB storage for Kernel Virtual Machines (KVM) application hosting and Linux container (LXC) hosting. The storage drive can also be used to save packet captures, trace logs generated by the operating system, GIR snapshots and third-party applications. The module connects to the USB 3.0 port on the rear panel of the device. For information about the hardware, see the Cisco Catalyst 9300 Series Switches Hardware Installation Guide.

Software Features in Cisco IOS XE Fuji 16.9.1

Feature Name	Description and License Level Information
AVC Switching: Export input and output interface information	• Support for two predefined directional wired Application Visibility and Control (WDAVC) Flexible NetFlow (FNF) records, ingress and egress, is introduced. • Support for attaching up to two different WDAVC FNF monitors with different records to an interface at the same time is enabled. See System Management → Configuring Application Visibility and Control in a Wired Network . (DNA Advantage)
Blue Beacon	The **show beacon all** privileged EXEC command is introduced; Use this command to display beacon LED status. See Interface and Hardware Commands . (Network Essentials and Network Advantage)
Display FPGA settings	The **show platform hardware fpga** priviledged EXEC command is introduced; Use this command to display system Field Programmable Gate Arrays (FPGA) settings. See System Management Commands .
Generic Online Diagnostics (GOLD)	The **TestUnusedPortLoopback** and **TestPortTxMonitoring** diagnostic test commands are introduced; Use these commands to test and verify hardware functionality. See System Management → Configuring Online Diagnostics . (Network Essentials and Network Advantage)

Feature Name	Description and License Level Information
Graceful Insertion and Removal (GIR) enhancements	These enhancements have been added the GIR feature: • Snapshot templates can now be used to generate specific snapshots. • Protocols belonging to one class within the same custom template are serviced in parallel. • System mode maintenance counters have been added to track several events such as the number of times the switch went into maintenance. See Stack Manager and High Availability → Configuring Graceful Insertion and Removal . (Network Advantage)
GIR Layer 2 protocol support for GIR Hot Standby Router Protocol (HSRP)	GIR is now supported for the HSRP protocol. See Stack Manager and High Availability → Configuring Graceful Insertion and Removal . (Network Advantage)
GIR Layer 2 protocol support for GIR Virtual Router Redundancy Protocol (VRRP)	GIR is now supported for the VRRP protocol. See Stack Manager and High Availability → Configuring Graceful Insertion and Removal . (Network Advantage)
Hot Patching Support	Allows Software Maintenance Upgrade (SMU) to happen immediately after activation, without reloading the system. See System Management → Software Maintenance Upgrade . (Network Advantage for CLI and DNA Advantage for DNAC)

Feature Name	Description and License Level Information
Media Access Control Security (MACsec) port channel support	Provides support for MACsec over port channels for Layer 2 and Layer 3 EtherChannels. See Security → MACsec Encryption . 128-bit—(Network Essentials and Network Advantage) 256-bit—(Network Advantage)
Media Access Control Security (MACsec): 256-bit AES MACsec (IEEE 802.1AE) host link encryption) with MACsec Key Agreement (MKA)	Support for 256-bit AES MACsec (IEEE 802.1AE) encryption with MACsec Key Agreement (MKA) on the downlink ports is enabled. See Security → MACsec Encryption . 256-bit—(Network Advantage)
MACsec Key Agreement (MKA) cipher announcement exchange	Support for cipher announcement is enabled. Cipher Announcement allows the supplicant and the authenticator to announce their respective MACsec Cipher Suite capabilities through EAPoL announcements. Two types of EAPoL announcements are supported – Secured announcements and unsecured announcements. See Security → MACsec Encryption . 128-bit—(Network Essentials and Network Advantage) 256-bit—(Network Advantage)
MACsec: XPN for 40 and 100 Gigabit Ethernet MACsec interfaces	The Extended Packet Numbering (XPN) feature in MKA or MACsec, eliminates the need for frequent secure association key (SAK) rekey that may occur in high capacity links (40 Gb/s, 100 Gb/s, and higher) and provides the option to use the GCM-AES-XPN-128 or GCM-AES-XPN-256 ciphersuites under the defined MKA policy. See Security → MACsec Encryption . 128-bit—(Network Essentials and Network Advantage) 256-bit—(Network Advantage)

Feature Name	Description and License Level Information
Network-Powered Lighting (Persistent PoE, Fast PoE, 2-event Classification, and Autosmart Ports	Enables network-powered lighting capability on a switch. It includes support for the following components: • Fast PoE—Remembers the last power drawn from a particular PSE port and switches on power the moment AC power is plugged in (within 15 to 20 seconds of switching on power) without waiting for Cisco IOS to boot up. • Perpetual-PoE—Provides uninterrupted power to a connected PD (Powered-Device) device even when the PSE (Power Sourcing Equipment), that is, the switch, is booting. • Two Event Classification for PoE—A physical layer mechanism to rapidly negotiate and grant PoE power to capable end-devices in less than 1sec without traditional Link Layer Discovery Protocol (LLDP) power negotiation. • Autosmart Ports—Provides endpoint specific macros to be triggered on detecting a lighting endpoint. See Network Powered Lighting . (Network Essentials and Network Advantage)
Open Shortest Path First version 3 (OSPFv3) Authentication Trailer	Provides a mechanism to authenticate OSPFv3 protocol packets as an alternative to existing OSPFv3 IPsec authentication. See Routing → Configuring OSPFv3 Authentication Trailer . (Network Advantage)

Feature Name	Description and License Level Information
Programmability	The following programmability features are introduced in this release: • Candidate Configuration—A temporary configuration that can be modified without changing running configuration. You can then choose when to update the device's configuration with the candidate configuration, by committing and confirming the candidate configuration. • OpenFlow 1.3 Multitable—Enables integration with open source Faucet SDN Controllers to automate management of layer 2 switching, VLANs, ACLs, and layer 3 routing (Network Essentials and Network Advantage) • YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1691. 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. • Zero Touch Provisioning (DHCPv6)—Dynamic Host Control Protocol Version 6 (DHCPv6) support is added to the Zero-touch provisioning feature in this release. DHCPv6 is enabled by default, and works on any device that boots without startup configuration. See Programmability Configuration Guide.
RadSec over TLS	RadSec over Transport Layer Security (TLS) is now supported on both client and device servers. See Security → Configuring RadSec. (Network Essentials and Network Advantage)
REP downlink support	Allows REP configuration on downlink ports. See Layer 2 → Configuring Resilient Ethernet Protocol. (Network Essentials and Network Advantage)

Feature Name	Description and License Level Information
Smart Licensing	A cloud-based, software license management solution that allows you to manage and track the status of your license, hardware, and software usage trends. **Note** Starting from this release, Smart Licensing is the default and the only available method to manage licenses. **Important** Starting from Cisco IOS XE Fuji 16.9.1 the Right-To-Use (RTU) licensing mode is deprecated, and the associated **license right-to-use** command is no longer available on the CLI. See the Cisco Smart Licensing, on page 36 section in this release note document and System Management → Configuring Smart Licensing in the configuration guide. A license level is not applicable.
Virtual Extensible LAN (VXLAN) Border Gateway Protocol (BGP) Ethernet VPN (EVPN)	A VXLAN is a network overlay that allows layer 2 segments to be stretched across an IP core. All the benefits of layer 3 topologies are thereby available with VXLAN. The overlay protocol is VXLAN and BGP uses EVPN as the address family for communicating end host MAC and IP addresses See Layer 2 → Configuring VXLAN BGP EVPN (Network Advantage)

New on the Web UI	
These features are introduced on the Web UI in this release	• Multicast—Minor improvements to configuring Internet Group Management Protocol (IGMP) snooping and to set the IGMP timeout. • Open Shortest Path First (OSPF)—Supports OSPF standards-based routing protocol for improved routing of data packets to their destination. • Quality of Service (QoS)—Supports QoS to make your network performance more predictable and bandwidth utilization more effective. • Site Profile—New site profiles for access, distributed, and core switches for easier initial configuration of the device. • Smart Licencing—Supports both online and offline method of license reservation to simplify and automate the management of licenses for your Cisco products. Smart Licensing on the device works with the Cisco Smart Software Manager (Cisco SSM). • Switched Port Analyzer (SPAN)—Supports SPAN to analyze network traffic passing through ports or VLANs.

Important Notes

Unsupported Features

- Bluetooth
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Converged Access for Branch Deployments
- Gateway Load Balancing Protocol (GLBP)
- IPsec VPN
- Performance Monitoring (PerfMon)
- Virtual Routing and Forwarding (VRF)-Aware web authentication

Complete List of Supported Features

For the complete list of features supported on a platform, see the Cisco Feature Navigator at https://www.cisco.com/go/cfn.

Accessing Hidden Commands

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

Hidden commands have always been present in Cisco IOS XE, but were not equipped with CLI help. This means that entering enter a question mark (?) at the system prompt did not display the list of available commands. Such hidden commands are only meant to assist Cisco TAC in advanced troubleshooting and are therefore not documented. For more information about CLI help, see the *Using the Command-Line Interface → Understanding the Help System* chapter of the Comman Reference document.

Hidden commands are available under:

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

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

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

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

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

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

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

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

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

Microcode Backward Compatibility When Downgrading

If you are downgrading the software version on your device from Cisco IOS XE Gibraltar 16.12.1 or a later release, to any of the following releases, the microcode must be downgraded:

- Cisco IOS XE Everest 16.6.1 through Cisco IOS XE Everest 16.6.6
- Cisco IOS XE Fuji 16.9.1 through Cisco IOS XE Fuji 16.9.2

If microcode downgrade does not occur, PoE features will be impacted after downgrading. See the Downgrading in Install Mode section of the *Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Gibraltar 16.12.x* for more information.

Supported Hardware

Cisco Catalyst 9300 Series Switches—Model Numbers

The following table lists the supported hardware models and the default license levels they are delivered with. For information about the available license levels, see section *License Levels* .

Table 1: Cisco Catalyst 9300 Series Switches

Switch Model	Default License Level[1]	Description
C9300-24P-A	Network Advantage	Stackable 24 10/100/1000 PoE+ ports; PoE budget of 437W; 715 WAC power supply; supports StackWise-480 and StackPower
C9300-24P-E	Network Essentials	
C9300-24T-A	Network Advantage	Stackable 24 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower
C9300-24T-E	Network Essentials	
C9300-24U-A	Network Advantage	Stackable 24 10/100/1000 UPoE ports; PoE budget of 830W; 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-24U-E	Network Essentials	
C9300-24UX-A	Network Advantage	Stackable 24 Multigigabit Ethernet 100/1000/2500/5000/10000 UPoE ports; PoE budget of 490 W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-24UX-E	Network Essentials	
C9300-48T-A	Network Advantage	Stackable 48 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower
C9300-48T-E	Network Essentials	
C9300-48P-A	Network Advantage	Stackable 48 10/100/1000 PoE+ ports; PoE budget of 437W; 715 WAC power supply; supports StackWise-480 and StackPower
C9300-48P-E	Network Essentials	
C9300-48T-A	Network Advantage	Stackable 48 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower
C9300-48T-E	Network Essentials	

Switch Model	Default License Level[1]	Description
C9300-48U-A	Network Advantage	Stackable 48 10/100/1000 UPoE ports; PoE budget of 822 W; 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-48U-E	Network Essentials	
C9300-48UN-A	Network Advantage	Stackable 48 Multigigabit Ethernet (100 Mbps or 1/2.5/5 Gbps) UPoE ports; PoE budget of 610 W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-48UN-E	Network Essentials	
C9300-48UXM-A	Network Advantage	Stackable 48 (36 2.5G Multigigabit Ethernet and 12 10G Multigigabit Ethernet Universal Power Over Ethernet (UPOE) ports)
C9300-48UXM-E	Network Essentials	

[1] See section *Licensing → Table: Permitted Combinations*, in this document for information about the add-on licenses that you can order.

Network Modules

The following table lists the optional uplink network modules with 1-Gigabit, 10-Gigabit, 25-Gigabit, and 40-Gigabit slots. You should only operate the switch with either a network module or a blank module installed.

Network Module	Description
C3850-NM-4-1G [1]	Four 1 Gigabit Ethernet SFP module slots
C3850-NM-2-10G [1]	Two 10 Gigabit Ethernet SFP module slots
C3850-NM-4-10G [1]	Four 10 Gigabit Ethernet SFP module slots
C3850-NM-8-10G [1]	Eight 10 Gigabit Ethernet SFP module slots
C3850-NM-2-40G [1]	Two 40 Gigabit Ethernet SFP module slots
C9300-NM-4G [2]	Four 1 Gigabit Ethernet SFP module slots
C9300-NM-4M [2]	Four MultiGigabit Ethernet slots
C9300-NM-8X [2]	Eight 10 Gigabit Ethernet SFP+ module slots

Network Module	Description
C9300-NM-2Q [2]	Two 40 Gigabit Ethernet QSFP+ module slots
C9300-NM-2Y [2]	Two 25 Gigabit Ethernet SFP28 module slots

Note

1. These network modules are supported only on the C3850 and C9300 SKUs of the Cisco Catalyst 3850 Series Switches and Cisco Catalyst 9300 Series Switches respectively.
2. These network modules are supported only on the C9300 SKUs of the Cisco Catalyst 9300 Series Switches.

Optics Modules

Cisco Catalyst Series Switches support a wide range of optics and the list of supported optics is updated on a regular basis. Use the Transceiver Module Group (TMG) Compatibility Matrix tool, or consult the tables at this URL for the latest transceiver module compatibility information: https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Compatibility Matrix

The following table provides software compatibility information.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Fuji 16.9.8	2.5 2.1	5.4 5.5	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.7	2.5 2.1	5.4 5.5	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.6	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.5	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Fuji 16.9.4	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.3	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.2	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.1	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.8.1a	2.3 Patch 1 2.4	5.4 5.5	PI 3.3 + PI 3.3 latest maintenance release + PI 3.3 latest device pack See Cisco Prime Infrastructure 3.3→ **Downloads**.
Everest 16.6.4a	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.4	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.3	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
Everest 16.6.2	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
Everest 16.6.1	2.2	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Everest 16.5.1a	2.1 Patch 3	5.4 5.5	-

Web UI System Requirements

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

Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[2]	512 MB[3]	256	1280 x 800 or higher	Small

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

Software Requirements

Operating Systems

- Windows 10 or later
- Mac OS X 10.9.5 or later

Browsers

- Google Chrome—Version 59 or later (On Windows and Mac)
- Microsoft Edge
- Mozilla Firefox—Version 54 or later (On Windows and Mac)
- Safari—Version 10 or later (On Mac)

Upgrading the Switch Software

This section covers the various aspects of upgrading or downgrading the device software.

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

Finding the Software Version

The package files for the Cisco IOS XE software are stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch.

Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the **dir** *filesystem:* privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Software Images

Release	Image Type	File Name
Cisco IOS XE Fuji 16.9.8	CAT9K_IOSXE	cat9k_iosxe.16.09.08.SPA.
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.08.S
Cisco IOS XE Fuji 16.9.7	CAT9K_IOSXE	cat9k_iosxe.16.09.07.SPA.
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.07.S
Cisco IOS XE Fuji 16.9.6	CAT9K_IOSXE	cat9k_iosxe.16.09.06.SPA.
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.06.S
Cisco IOS XE Fuji 16.9.5	CAT9K_IOSXE	cat9k_iosxe.16.09.05.SPA.
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.05.S
Cisco IOS XE Fuji 16.9.4	CAT9K_IOSXE	cat9k_iosxe.16.09.04.SPA.
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.04.S
Cisco IOS XE Fuji 16.9.3	CAT9K_IOSXE	cat9k_iosxe.16.09.03.SPA.
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.03.S
Cisco IOS XE Fuji 16.9.2	CAT9K_IOSXE	cat9k_iosxe.16.09.02.SPA.
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.02.S

Release	Image Type	File Name
Cisco IOS XE Fuji 16.9.1	CAT9K_IOSXE	cat9k_iosxe.16.09.01.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.01.SPA

Automatic Boot Loader Upgrade

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

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

⚠

Caution Do not power cycle your switch during the upgrade.

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE Fuji 16.9.1 or Cisco IOS XE Fuji 16.9.2 or Cisco IOS XE Fuji 16.9.3 or Cisco IOS XE Fuji 16.9.4 or Cisco IOS XE Fuji 16.9.5 or Cisco IOS XE Fuji 16.9.6 or Cisco IOS XE Fuji 16.9.7 or Cisco IOS XE Fuji 16.9.8for the first time.	The boot loader may be upgraded to version 16.9.1r [FC3], For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 16.9.1r [FC3], RELEASE SOFTWARE (P)`
	If the automatic boot loader upgrade occurs, while booting Cisco IOS XE Fuji 16.9.1 or Cisco IOS XE Fuji 16.9.2 or Cisco IOS XE Fuji 16.9.3 Cisco IOS XE Fuji 16.9.4 or Cisco IOS XE Fuji 16.9.5 or Cisco IOS XE Fuji 16.9.6, you will see the following on the console:
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Thu Mar 14 19:03:28 Universal 2018 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`waiting for upgrades to complete...`

Automatic Microcode Upgrade

During a Cisco IOS image upgrade or downgrade on a PoE or UPoE switch, the microcode is updated to reflect applicable feature enhancements and bug fixes. Do not restart the switch during the upgrade or downgrade process.

It takes approximately an additional 4 minutes to complete the microcode upgrade in addition to the normal reload time; however, data traffic continues to be forwarded during the upgrade. The microcode update occurs only during an image upgrade or downgrade on PoE or UPoE switches. It does not occur during switch reloads or on non-PoE switches.

The following console messages are displayed during microcode upgrade.

```
MM [1] MCU version 111 sw ver 105
MM [2] MCU version 111 sw ver 105

Front-end Microcode IMG MGR: found 4 microcode images for 1 device.
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_0 mismatch: 0
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_1 mismatch: 1
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_2 mismatch: 1
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_3 mismatch: 0

Front-end Microcode IMG MGR: Preparing to program device microcode...
Front-end Microcode IMG MGR: Preparing to program device[0], index=0 ...594412 bytes....
Skipped[0].
Front-end Microcode IMG MGR: Preparing to program device[0], index=1 ...393734 bytes.
Front-end Microcode IMG MGR: Programming device 0...rwRrrrrrrw..
0%.....................................................................
10%.....................................................................
20%.....................................................................
30%.....................................................................
40%.....................................................................
50%.....................................................................
60%.....................................................................
70%.....................................................................
80%.....................................................................
90%.....................................................................100%
Front-end Microcode IMG MGR: Preparing to program device[0], index=2 ...25186 bytes.
Front-end Microcode IMG MGR: Programming device
0...rrrrrrw..0%....10%....20%......30%...40%......50%....60%......70%...80%......90%....100%wRr!
Front-end Microcode IMG MGR: Microcode programming complete for device 0.
Front-end Microcode IMG MGR: Preparing to program device[0], index=3 ...86370 bytes....
Skipped[3].
Front-end Microcode IMG MGR: Microcode programming complete in 290 seconds
```

Software Installation Commands

Summary of Software Installation Commands **Supported starting from Cisco IOS XE Everest 16.6.2 and later releases**	
To install and activate the specified file, and to commit changes to be persistent across reloads: **install add file** *filename* [**activate commit**] To separately install, activate, commit, cancel, or remove the installation file: **install ?**	
add file tftp: *filename*	Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.
activate [**auto-abort-timer**]	Activates the file, and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Note The **request platform software** commands are deprecated starting from Cisco IOS XE Gibraltar 16.10.1. The commands are visible on the CLI in this release and you can configure them, but we recommend that you use the **install** commands to upgrade or downgrade.

Summary of request platform software Commands	
`Device# request platform software package ?`	
clean	Cleans unnecessary package files from media
copy	Copies package to media
describe	Describes package content
expand	Expands all-in-one package to media
install	Installs the package
uninstall	Uninstalls the package
verify	Verifies In Service Software Upgrade (ISSU) software package compatibility

Upgrading in Install Mode

Follow these instructions to upgrade from one release to another, in install mode.

Before you begin

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

When upgrading from ...	Use these commands...	To upgrade to...
Cisco IOS XE Everest 16.5.1a or Cisco IOS XE Everest 16.6.1	Only **request platform software** commands	Cisco IOS XE Fuji 16.9.x
Cisco IOS XE Everest 16.6.2 and later	Either **install** commands or **request platform software** commands	

The sample output in this section displays upgrade from

- Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Fuji 16.9.1 using **request platform software** commands.
- Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Fuji 16.9.1 using **install** commands.

Procedure

Step 1 Clean Up

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.

- **request platform software package clean**
- **install remove inactive**

The following sample output displays the cleaning up of unused files, by using the **request platform software package clean** command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Fuji 16.9.1. Use the **switch all** option to clean up all the switches in your stack

Note Ignore the hexdump: messages in the CLI when you enter the command; they have no functional impact and will be removed in a later release. You will see this only on member switches and not on the active or standby. In the sample output below, hexdump messages are seen on switch 3, which is a member switch.

```
Switch# request platform software package clean switch all
Running command on switch 1
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.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.
done.

Running command on switch 2
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.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
```

```
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.

Running command on switch 3
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 ...
hexdump: NVRAM: No such file or directory
hexdump: all input file arguments failed
head: cannot open 'NVRAM' for reading: No such file or directory
NVRAM: No such file or directory
hexdump: NVRAM: No such file or directory
hexdump: stdin: Bad file descriptor
tail: cannot open 'NVRAM' for reading: No such file or directory
hexdump: NVRAM: No such file or directory
hexdump: all input file arguments failed
cat9k-cc_srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.

The following files will be deleted:
[1]:
/flash/cat9k-cc_srdriver.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
```

```
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-
[2]:
/flash/cat9k-cc_srdriver.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-
[3]:
/flash/cat9k-cc_srdriver.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-

Do you want to proceed? [y/n]y
[1]:
Deleting file flash:cat9k-cc_srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-webui.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[2]:
Deleting file flash:cat9k-cc_srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-webui.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[3]:
Deleting file flash:cat9k-cc_srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.SPA.pkg ... done.
```

```
Deleting file flash:cat9k-webui.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted
```

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command, for upgrade scenario Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Fuji 16.9.1:

```
Switch# install remove inactive
install_remove: START Tue Jul 10 19:51:48 UTC 2018
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.16.06.03.SPA.pkg
/flash/cat9k-espbase.16.06.03.SPA.pkg
/flash/cat9k-guestshell.16.06.03.SPA.pkg
/flash/cat9k-rpbase.16.06.03.SPA.pkg
/flash/cat9k-rpboot.16.06.03.SPA.pkg
/flash/cat9k-sipbase.16.06.03.SPA.pkg
/flash/cat9k-sipspa.16.06.03.SPA.pkg
/flash/cat9k-srdriver.16.06.03.SPA.pkg
/flash/cat9k-webui.16.06.03.SPA.pkg
/flash/cat9k-wlc.16.06.03.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.06.03.SPA.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
[1] Post_Remove_Cleanup package(s) on switch 1
[1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Tue Jul 10 19:52:25 UTC 2018
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.09.01.SPA.bin flash:
Destination filename [cat9k_iosxe.16.09.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.09.01.SPA.bin...
```

```
Loading /cat9k_iosxe.16.09.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]

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

b) **dir flash**

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

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

Directory of flash:/

434184 -rw- 601216545 Jul 10 2018 10:18:11 -07:00 cat9k_iosxe.16.09.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

Step 3 Set boot variable

a) **boot system flash:packages.conf**

Use this command to set the boot variable to **flash:packages.conf**.

```
Switch(config)# boot system flash:packages.conf
Switch(config)# exit
```

b) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

c) **show boot system**

Use this command to verify the boot variable is set to **flash:packages.conf** and the manual boot variable is set to **no**.

The output should display **BOOT variable** = **flash:packages.conf**.

```
Switch# show boot system
```

Step 4 Software install image to flash

- **request platform software package install**
- **install add file activate commit**

You can point to the source image on your TFTP server or in flash if you have it copied to flash. We recommend copying the image to a TFTP server or the flash drive of the active switch. If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For example, if the image is on the flash drive of member switch 3 (flash-3):

```
Switch# request platform software package install switch all file
flash-3:cat9k_iosxe.16.09.01.SPA.bin auto-copy.
```

The following sample output displays installation of the Cisco IOS XE Fuji 16.9.1 software image to flash, by using the **request platform software package install** command, for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Fuji 16.9.1.

```
Switch# request platform software package install switch all file
flash:cat9k_iosxe.16.09.01.SPA.bin auto-copy
```

```
--- Starting install local lock acquisition on switch 1 ---
Finished install local lock acquisition on switch 1

Expanding image file: flash:cat9k_iosxe.16.09.01.SPA.bin
[1]: Copying flash:cat9k_iosxe.16.09.01.SPA.bin from switch 1 to switch 2 3
[2 3]: Finished copying to switch 2 3
[1 2 3]: Expanding file
[1 2 3]: Finished expanding all-in-one software package in switch 1 2 3
SUCCESS: Finished expanding all-in-one software package.
[1 2 3]: Performing install
SUCCESS: install finished
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
Removed cat9k-sipbase.16.05.01a.SPA.pkg
Removed cat9k-sipspa.16.05.01a.SPA.pkg
Removed cat9k-srdriver.16.05.01a.SPA.pkg
Removed cat9k-webui.16.05.01a.SPA.pkg
Removed cat9k-wlc.16.05.01a.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.09.01.SPA.pkg
Added cat9k-espbase.16.09.01.SPA.pkg
Added cat9k-guestshell.16.09.01.SPA.pkg
Added cat9k-rpbase.16.09.01.SPA.pkg
Added cat9k-rpboot.16.09.01.SPA.pkg
Added cat9k-sipbase.16.09.01.SPA.pkg
Added cat9k-sipspa.16.09.01.SPA.pkg
Added cat9k-srdriver.16.09.01.SPA.pkg
Added cat9k-webui.16.09.01.SPA.pkg
Added cat9k-wlc.16.09.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[1]: Finished install successful on switch 1
[2]: install package(s) on switch 2
--- Starting list of software package changes ---
Old files list:
Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
Removed cat9k-sipbase.16.05.01a.SPA.pkg
Removed cat9k-sipspa.16.05.01a.SPA.pkg
Removed cat9k-srdriver.16.05.01a.SPA.pkg
Removed cat9k-webui.16.05.01a.SPA.pkg
Removed cat9k-wlc.16.05.01a.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.09.01.SPA.pkg
Added cat9k-espbase.16.09.01.SPA.pkg
Added cat9k-guestshell.16.09.01.SPA.pkg
Added cat9k-rpbase.16.09.01.SPA.pkg
Added cat9k-rpboot.16.09.01.SPA.pkg
Added cat9k-sipbase.16.09.01.SPA.pkg
Added cat9k-sipspa.16.09.01.SPA.pkg
Added cat9k-srdriver.16.09.01.SPA.pkg
Added cat9k-webui.16.09.01.SPA.pkg
Added cat9k-wlc.16.09.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
```

```
[2]: Finished install successful on switch 2
[3]: install package(s) on switch 3
--- Starting list of software package changes ---
Old files list:
Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
Removed cat9k-sipbase.16.05.01a.SPA.pkg
Removed cat9k-sipspa.16.05.01a.SPA.pkg
Removed cat9k-srdriver.16.05.01a.SPA.pkg
Removed cat9k-webui.16.05.01a.SPA.pkg
Removed cat9k-wlc.16.05.01a.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.09.01.SPA.pkg
Added cat9k-espbase.16.09.01.SPA.pkg
Added cat9k-guestshell.16.09.01.SPA.pkg
Added cat9k-rpbase.16.09.01.SPA.pkg
Added cat9k-rpboot.16.09.01.SPA.pkg
Added cat9k-sipbase.16.09.01.SPA.pkg
Added cat9k-sipspa.16.09.01.SPA.pkg
Added cat9k-srdriver.16.09.01.SPA.pkg
Added cat9k-webui.16.09.01.SPA.pkg
Added cat9k-wlc.16.09.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[3]: Finished install successful on switch 3
Checking status of install on [1 2 3]
[1 2 3]: Finished install in switch 1 2 3
SUCCESS: Finished install: Success on [1 2 3]
```

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

The following sample output displays installation of the Cisco IOS XE Fuji 16.9.1 software image to flash, by using the **install add file activate commit** command, for upgrade scenario Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Fuji 16.9.1:

```
Switch# install add file flash:cat9k_iosxe.16.09.01.SPA.bin activate commit

install_add_activate_commit: START Tue Jul 10 19:54:51 UTC 2018

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]y
Building configuration...

[OK]Modified configuration has been saved

*Jul 10 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 10 19:54:55 install_engine.sh:

%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.09.01.SPA.bininstall_add_activate_commit: Adding PACKAGE

This operation requires a reload of the system. Do you want to proceed?
Please confirm you have changed boot config to flash:packages.conf [y/n]y

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.09.01.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
Following packages shall be activated:
/flash/cat9k-wlc.16.09.01.SPA.pkg
/flash/cat9k-webui.16.09.01.SPA.pkg
/flash/cat9k-srdriver.16.09.01.SPA.pkg
/flash/cat9k-sipspa.16.09.01.SPA.pkg
/flash/cat9k-sipbase.16.09.01.SPA.pkg
/flash/cat9k-rpboot.16.09.01.SPA.pkg
/flash/cat9k-rpbase.16.09.01.SPA.pkg
/flash/cat9k-guestshell.16.09.01.SPA.pkg
/flash/cat9k-espbase.16.09.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.09.01.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

*Jul 10 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 10 19:57:41 rollback_timer.sh:

%INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Install auto abort timer will expire in 7200
 seconds [1] Commit package(s) on switch 1
[1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit Tue Jul 10 19:57:48 UTC 2017
Switch#
```

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

If you choose to not reload the system by entering **n**, when prompted with the message `This operation requires a reload of the system. Do you want to proceed? [y/n]`, follow the steps 1 and 2 below to avoid any boot issues during the next or subsequent reloads.

a) **install activate**

Use this command to activate the installed image.

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

```
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate
Install will reload the system now!
SUCCESS: install_activate Fri Mar 22 19:57:48 UTC 2019
```

b) **install commit**

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

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

install_commit: Committing PACKAGE

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

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

Step 5 **dir flash:**

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

The following is sample output of the **dir flash:** command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Fuji 16.9.1:

```
Switch# dir flash:*.pkg

Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104   Jul 26 2017 09:52:41 -07:00 cat9k-cc_srdriver.16.05.01a.SPA.pkg
475141 -rw- 70333380  Jul 26 2017 09:52:44 -07:00 cat9k-espbase.16.05.01a.SPA.pkg
475142 -rw- 13256     Jul 26 2017 09:52:44 -07:00 cat9k-guestshell.16.05.01a.SPA.pkg
475143 -rw- 349635524 Jul 26 2017 09:52:54 -07:00 cat9k-rpbase.16.05.01a.SPA.pkg
475149 -rw- 24248187  Jul 26 2017 09:53:02 -07:00 cat9k-rpboot.16.05.01a.SPA.pkg
475144 -rw- 25285572  Jul 26 2017 09:52:55 -07:00 cat9k-sipbase.16.05.01a.SPA.pkg
475145 -rw- 20947908  Jul 26 2017 09:52:55 -07:00 cat9k-sipspa.16.05.01a.SPA.pkg
475146 -rw- 2962372   Jul 26 2017 09:52:56 -07:00 cat9k-srdriver.16.05.01a.SPA.pkg
475147 -rw- 13284288  Jul 26 2017 09:52:56 -07:00 cat9k-webui.16.05.01a.SPA.pkg
475148 -rw- 13248     Jul 26 2017 09:52:56 -07:00 cat9k-wlc.16.05.01a.SPA.pkg

491524 -rw- 25711568  Jul 10 2018 11:49:33 -07:00  cat9k-cc_srdriver.16.09.01.SPA.pkg
491525 -rw- 78484428  Jul 10 2018 11:49:35 -07:00  cat9k-espbase.16.09.01.SPA.pkg
491526 -rw- 1598412   Jul 10 2018 11:49:35 -07:00  cat9k-guestshell.16.09.01.SPA.pkg
491527 -rw- 404153288 Jul 10 2018 11:49:47 -07:00  cat9k-rpbase.16.09.01.SPA.pkg
491533 -rw- 31657374  Jul 10 2018 11:50:09 -07:00  cat9k-rpboot.16.09.01.SPA.pkg
491528 -rw- 27681740  Jul 10 2018 11:49:48 -07:00  cat9k-sipbase.16.09.01.SPA.pkg
491529 -rw- 52224968  Jul 10 2018 11:49:49 -07:00  cat9k-sipspa.16.09.01.SPA.pkg
491530 -rw- 31130572  Jul 10 2018 11:49:50 -07:00  cat9k-srdriver.16.09.01.SPA.pkg
491531 -rw- 14783432  Jul 10 2018 11:49:51 -07:00  cat9k-webui.16.09.01.SPA.pkg
491532 -rw- 9160      Jul 10 2018 11:49:51 -07:00  cat9k-wlc.16.09.01.SPA.pkg
```

```
11353194496 bytes total (8963174400 bytes free)
```

The following is sample output of the **dir flash:** command for the Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Fuji 16.9.1 upgrade scenario:

```
Switch# dir flash:

Directory of flash:/

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

491524 -rw- 25711568  Jul 10 2018 11:49:33 -07:00  cat9k-cc_srdriver.16.09.01.SPA.pkg
491525 -rw- 78484428  Jul 10 2018 11:49:35 -07:00  cat9k-espbase.16.09.01.SPA.pkg
491526 -rw- 1598412   Jul 10 2018 11:49:35 -07:00  cat9k-guestshell.16.09.01.SPA.pkg
491527 -rw- 404153288 Jul 10 2018 11:49:47 -07:00  cat9k-rpbase.16.09.01.SPA.pkg
491533 -rw- 31657374  Jul 10 2018 11:50:09 -07:00  cat9k-rpboot.16.09.01.SPA.pkg
491528 -rw- 27681740  Jul 10 2018 11:49:48 -07:00  cat9k-sipbase.16.09.01.SPA.pkg
491529 -rw- 52224968  Jul 10 2018 11:49:49 -07:00  cat9k-sipspa.16.09.01.SPA.pkg
491530 -rw- 31130572  Jul 10 2018 11:49:50 -07:00  cat9k-srdriver.16.09.01.SPA.pkg
491531 -rw- 14783432  Jul 10 2018 11:49:51 -07:00  cat9k-webui.16.09.01.SPA.pkg
491532 -rw- 9160      Jul 10 2018 11:49:51 -07:00  cat9k-wlc.16.09.01.SPA.pkg

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

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

- packages.conf—the file that has been re-written with the newly installed .pkg files
- packages.conf.00—backup file of the previously installed image
- cat9k_iosxe.16.09.01.SPA.conf— a copy of packages.conf and not used by the system.

```
Switch# dir flash:*.conf

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

434197 -rw- 7406 Jul 10 2018 10:59:16 -07:00 packages.conf
434196 -rw- 7504 Jul 10 2018 10:59:16 -07:00 packages.conf.00-
516098 -rw- 7406 Jul 10 2018 10:58:08 -07:00 cat9k_iosxe.16.09.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

Step 6 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

If your switches are configured with auto boot, then the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
Switch: boot flash:packages.conf
```

c) **show version**

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

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

The following sample output of the **show version** command displays the Cisco IOS XE Fuji 16.9.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.09.01

Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.1,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2018 by Cisco Systems, Inc.

Compiled Tue 10-Jul-18 07:45 by mcpre
```

Downgrading in Install Mode

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

Before you begin

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

When downgrading from ...	Use these commands...	To downgrade to...
Cisco IOS XE Fuji 16.9.5 or Cisco IOS XE Fuji 16.9.4 or Cisco IOS XE Fuji 16.9.3 or Cisco IOS XE Fuji 16.9.2 or Cisco IOS XE Fuji 16.9.1	Either **install** commands or **request platform software** commands	Cisco IOS XE Fuji 16.9.x or Cisco IOS XE Fuji 16.8.x or Cisco IOS XE Everest 16.x.x.

The sample output in this section shows downgrade from Cisco IOS XE Fuji 16.9.1 to Cisco IOS XE Everest 16.6.1, by using the **install** commands.

Important New switch models that are introduced in a release cannot be downgraded. For instance, if a new model is first introduced in Cisco IOS XE Fuji 16.8.1a, this is the minimum software version for the model. If you add a new switch to an existing stack, we recommend upgrading all existing switches to the latest release.

Procedure

Step 1 Clean Up

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.

- **request platform software package clean**
- **install remove inactive**

The following sample output displays the cleaning up of Cisco IOS XE Fuji 16.9.1 files using the **install remove inactive** command:

```
Switch# install remove inactive

install_remove: START Tue Jul 10 19:51:48 UTC 2018
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.16.09.01.SPA.pkg
/flash/cat9k-espbase.16.09.01.SPA.pkg
/flash/cat9k-guestshell.16.09.01.SPA.pkg
/flash/cat9k-rpbase.16.09.01.SPA.pkg
/flash/cat9k-rpboot.16.09.01.SPA.pkg
/flash/cat9k-sipbase.16.09.01.SPA.pkg
/flash/cat9k-sipspa.16.09.01.SPA.pkg
/flash/cat9k-srdriver.16.09.01.SPA.pkg
/flash/cat9k-webui.16.09.01.SPA.pkg
/flash/cat9k-wlc.16.09.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.09.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.09.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.09.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.09.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.09.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.09.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.09.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.09.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.09.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.09.01.SPA.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.

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

SUCCESS: install_remove Tue Jul 10 19:52:25 UTC 2018
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat9k_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)
```

b) **dir flash:**

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

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

Directory of flash:/

434184 -rw- 508584771 Jul 10 2018 13:35:16 -07:00 cat9k_iosxe.16.06.01.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Downgrade software image

- **install add file activate commit**
- **request platform software package install**

The following example displays the installation of the Cisco IOS XE Everest 16.6.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.16.06.01.SPA.bin activate commit

install_add_activate_commit: START Tue Jul 10 19:54:51 UTC 2018

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]yBuilding
 configuration...

[OK]Modified configuration has been saved

*Jul 10 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 10 19:54:55 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

This operation requires a reload of the system. Do you want to proceed?
Please confirm you have changed boot config to flash:packages.conf [y/n]y

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_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
Following packages shall be activated:
/flash/cat9k-wlc.16.06.01.SPA.pkg
/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

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

*Jul 10 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 10 19:57:41 rollback_timer.sh:
 %INSTALL-
5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Install auto abort timer will expire in 7200 seconds
[1] Commit package(s) on switch 1
[1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit Tue Jul 10 19:57:48 UTC 2018
Switch#
```

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

Step 4 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

If your switches are configured with auto boot, then the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
Switch: boot flash:packages.conf
```

Note When you downgrade the software image, the boot loader will not automatically downgrade. It will remain updated.

c) **show version**

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

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

The following sample output of the **show version** command displays the Cisco IOS XE Everest 16.6.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.06.01
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Fri 16-Mar-18 06:38 by mcpre
<output truncated>
```

Licensing

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

License Levels

The software features available on Cisco Catalyst 9300 Series Switches fall under these base or add-on license levels.

Base Licenses

- Network Essentials
- Network Advantage—Includes features available with the Network Essentials license and more.

Add-On Licenses

Add-On Licenses require a Network Essentials or Network Advantage as a pre-requisite. The features available with add-on license levels provide Cisco innovations on the switch, as well as on the Cisco Digital Network Architecture Center (Cisco DNA Center).

- DNA Essentials
- DNA Advantage— Includes features available with the DNA Essentials license and more.

To find information about platform support and to know which license levels a feature is available with, use Cisco Feature Navigator. To access Cisco Feature Navigator, go to https://cfnng.cisco.com. An account on cisco.com is not required.

License Types

The following license types are available:

- Permanent—for a license level, and without an expiration date.
- Term—for a license level, and for a three, five, or seven year period.
- Evaluation—a license that is not registered.

License Levels - Usage Guidelines

- Base licenses (Network Essentials and Network-Advantage) are ordered and fulfilled only with a permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a term license type.
- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- When ordering an add-on license with a base license, note the combinations that are permitted and those that are not permitted:

Table 2: Permitted Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No
Network Advantage	Yes[4]	Yes

[4] You will be able to purchase this combination only at the time of the DNA license renewal and not when you purchase DNA-Essentials the first time.

- Evaluation licenses cannot be ordered. They are not tracked via Cisco Smart Software Manager and expire after a 90-day period. Evaluation licenses can be used only once on the switch and cannot be regenerated. Warning system messages about an evaluation license expiry are generated only 275 days after expiration and every week thereafter. An expired evaluation license cannot be reactivated after reload. This applies only to *Smart Licensing*. The notion of evaluation licenses does not apply to *Smart Licensing Using Policy*.

Cisco Smart Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- Unified Management: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.

- License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (http://software.cisco.com).

Important Cisco Smart Licensing is the default and the only available method to manage licenses.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Deploying Smart Licensing

The following provides a process overview of a day 0 to day N deployment directly initiated from a device that is running Cisco IOS XE Fuji 16.9.1 or later releases. Links to the configuration guide provide detailed information to help you complete each one of the smaller tasks.

Procedure

Step 1 Begin by establishing a connection from your network to Cisco Smart Software Manager on cisco.com.

In the software configuration guide of the required release, see *System Management → Configuring Smart Licensing → Connecting to CSSM*

Step 2 Create and activate your Smart Account, or login if you already have one.

To create and activate Smart Account, go to Cisco Software Central → Create Smart Accounts. Only authorized users can activate the Smart Account.

Step 3 Complete the Cisco Smart Software Manager set up.

a) Accept the Smart Software Licensing Agreement.

b) Set up the required number of Virtual Accounts, users and access rights for the virtual account users.

Virtual accounts help you organize licenses by business unit, product type, IT group, and so on.

c) Generate the registration token in the Cisco Smart Software Manager portal and register your device with the token.

In the software configuration guide of the required release, see *System Management → Configuring Smart Licensing → Registering the Device in CSSM*

With this,

- The device is now in an authorized state and ready to use.
- The licenses that you have purchased are displayed in your Smart Account.

How Upgrading or Downgrading Software Affects Smart Licensing

Starting from Cisco IOS XE Fuji 16.9.1, Smart Licensing is the default and only license management solution; all licenses are managed as Smart Licenses.

Important Starting from Cisco IOS XE Fuji 16.9.1, the Right-To-Use (RTU) licensing mode is deprecated, and the associated **license right-to-use** command is no longer available on the CLI.

Note how upgrading to a release that supports Smart Licensing or moving to a release that does not support Smart Licensing affects licenses on a device:

- **When you upgrade from an earlier release to one that supports Smart Licensing**—all existing licenses remain in evaluation mode until registered in Cisco Smart Software Manager. After registration, they are made available in your Smart Account.

  In the software configuration guide of the required release, see *System Management → Configuring Smart Licensing → Registering the Device in CSSM*

- **When you downgrade to a release where Smart Licensing is not supported**—all smart licenses on the device are converted to traditional licenses and all smart licensing information on the device is removed.

Using Smart Licensing on an Out-of-the-Box Device

Starting from Cisco IOS XE Fuji 16.9.1, if an out-of-the-box device has the software version factory-provisioned, all licenses on such a device remain in evaluation mode until registered in Cisco Smart Software Manager.

In the software configuration guide of the required release, see *System Management → Configuring Smart Licensing → Registering the Device in CSSM*

Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst 9300 Series Switches datasheet at:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.html

Limitations and Restrictions

- Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
- Control Plane Policing (CoPP)—The show run command does not display information about classes configured under system-cpp policy, when they are left at default values. Use the show policy-map system-cpp-policy or the show policy-map control-plane commands in privileged EXEC mode instead.
- Flexible NetFlow limitations:
  - You cannot configure NetFlow export using the Ethernet Management port (GigabitEthernet0/0).
  - You can not configure a flow monitor on logical interfaces, such as switched virtual interfaces (SVIs), port-channel, loopback, tunnels.

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

- QoS restrictions:
    - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
    - For QoS policies, only switched virtual interfaces (SVI) are supported for logical interfaces.
    - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.
    - Stack Queuing and Scheduling (SQS) drops CPU bound packets exceeding 1.4 Gbps.

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

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

- Stacking:
    - A switch stack supports up to eight stack members.
    - Mixed stacking is not supported. Cisco Catalyst 9300 Series Switches cannot be stacked with Cisco Catalyst 3850 Series Switches.
    - Auto upgrade for a new member switch is supported only in the install mode.

- VLAN Restriction—It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.

- Wired Application Visibility and Control limitations:
    - NBAR2 (QoS and Protocol-discovery) configuration is allowed only on wired physical ports. It is not supported on virtual interfaces, for example, VLAN, port channel nor other logical interfaces.
    - NBAR2 based match criteria ‘match protocol’ is allowed only with marking or policing actions. NBAR2 match criteria will not be allowed in a policy that has queuing features configured.
    - ‘Match Protocol’: up to 256 concurrent different protocols in all policies.
    - NBAR2 and Legacy NetFlow cannot be configured together at the same time on the same interface. However, NBAR2 and wired AVC Flexible NetFlow can be configured together on the same interface.
    - Only IPv4 unicast (TCP/UDP) is supported.
    - AVC is not supported on management port (Gig 0/0)

- NBAR2 attachment should be done only on physical access ports. Uplink can be attached as long as it is a single uplink and is not part of a port channel.
- Performance—Each switch member is able to handle 2000 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.
- Scale—Able to handle up to 20000 bi-directional flows per 24 access ports and per 48 access ports.

- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.
- The File System Check (fsck) utility is not supported in install mode.

Caveats

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

Cisco Bug Search Tool

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

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

Open Caveats in Cisco IOS XE Fuji 16.9.x

Identifier	Description
CSCvi56567	When 9300 switch boots up, link up of its downlink has delayed if switch has network module
CSCvm79234	Show version cli shows invalid USB-SSD disk size on a CAT9k switch
CSCvq22224	cat9k // evpn/vxlan // dhcp relay not working over l3vni
CSCvs55409	Ethernet Trailer or additional bytes are added by 9300 in GRE Tunnel
CSCvi56567	When 9300 switch boots up, link up of its downlink has delayed if switch has network module
CSCvn55969	FED crash when 'show tech nbar' is run
CSCvq24181	Crash/Unresponsiveness after TDR test is set through SNMP
CSCvr90465	MACSEC link does not recover upon link flap
CSCvs15759	DHCP server sends out a NAK packet during DHCP renewal process.

Resolved Caveats in Cisco IOS XE Fuji 16.9.8

Caveat ID Number	Description
CSCvt53563	Cisco IOS XE Software NETCONF and RESTCONF Authentication Bypass Vulnerability
CSCvt88722	Keep auto-neg enabled even with hard code speed and duplex causing auto-neg mismatch
CSCvu90882	Romvar: Bootloop if SWITCH_DISABLE_PASSWORD_RECOVERY and SWITCH_IGNORE_STARTUP_CFG are both set to 1
CSCvv12527	Crash in SNMP Engine process while polling chassis id in lldp
CSCvw46194	IOS and IOS XE Software UDLD Denial of Service Vulnerability
CSCvx08994	CTS credential password will be added to local keystore even if the password is longer than 24 char
CSCvx34341	Netfilter: Linux Kernel triggers crash by race condition through delete operation
CSCvx41294	High CPU usage caused by "TCP Timer" process
CSCvx55976	Switch stack crash with FIPS mode enabled
CSCvx66699	Cisco IOS and IOS XE Software TrustSec CLI Parser Denial of Service Vulnerability
CSCvy17757	A crash due to issue with internal QOS policy specfic to EPC
CSCvy91786	C9300-24UX intermittently fails to pass traffic to Voice Gateways VG224 on 16.9.6 after reload

Resolved Caveats in Cisco IOS XE Fuji 16.9.7

Caveat ID Number	Description
CSCvn22162	Cat3k crash from corruption in AVL tree
CSCvu35094	Switch reloads due to fed crash after sending multicast data packets in pvlan

Resolved Caveats in Cisco IOS XE Fuji 16.9.6

Caveat ID Number	Description
CSCvn98703	FED_QOS_ERRMSG-3-POLICER_HW_ERROR on Catalysts switches running 16.6 releases
CSCvo31350	Cpu-interface queues may display a negative value for retrieved packets
CSCvq17488	show module info for active switch is n/a after booting remaining switches
CSCvq23523	Remove "request platform software trace rotate all" from show tech

Caveat ID Number	Description
CSCvq89352	cat9300: missing system_report when crashed
CSCvr37805	Cat3k/9k: Device might reboot after applying "mac address-static xxxx.xxxx.xxxx vlan x drop" command
CSCvr92287	EPC with packet-len opt breaks CPU in-band path for bigger frames
CSCvs50391	FED crash when premature free of SG element
CSCvs71084	Cat9k - Not able to apply Et-analytics on an interface
CSCvs71519	Switch reloads due to dhcp snooping
CSCvs75010	Traffic forwarding stops when Session Idle time out is configured 10 sec with active traffic running
CSCvs91195	Crash Due to AutoSmart Port Macros
CSCvs91593	offer is dropped in data vlan with dhcp snooping using dot1x/mab
CSCvt02962	Uplink Port-channel Trunk member link Port LED truns to amber blinking after link down/up
CSCvt13518	QoS ACL matching incorrectly when udp range is used
CSCvt70277	Power allocation issue in 16.9.x/16.12.x
CSCvt83025	Memory utilization increasing under fman_fp_image due to WRC Stats Req
CSCvu13029	Intermittent Link Flaps on mGig Cat9300 switches to mGig capable endpoints
CSCvu15007	Crash when invalid input interrupts a role-based access-list policy installation
CSCvu24011	Interface Not Passing Traffic after Boot-up with IE 3400 with forced speed/duplex setting on IE
CSCvu37176	SPAN filter cannot work well when configure FSPAN after 5th session.
CSCvu47903	First packet in native multicast flow drops due to RPF failure
CSCvu65433	Cat9300 stack member 'platform_mgr' process crash on obfl poe sensor handler

Resolved Caveats in Cisco IOS XE Fuji 16.9.5

Identifier	Description
CSCvk47894	Cat3k/9k SPAN monitor session works in stack only on adding 2 dest ports in stack
CSCvm66787	C9300 Fan speed increases when AC power removed from one FEP
CSCvm72574	16.6.4 CPP Police rate wrong in "class system-cpp-police-control-low-priority"
CSCvo56403	Standby Switch Stuck in HA Sync config after Stack-Merge

Identifier	Description
CSCvo81311	FMAN-RP crash observed on Guest Anchor
CSCvp84502	ERSPAN destination does not work or forward traffic
CSCvq05337	Cat3k/9k EGR_INVALID_REWRITE counter increasing in mVPN setup
CSCvq22011	IOS-XE drops ARP reply when IPDT gleans from ARP
CSCvq26295	cat9300: missing system_report when crashed
CSCvq38901	Enable CDP - removed on shut/ no shut dot1Q-tunnel interface
CSCvq44397	Cat3k/9k Ospf down upon switchover with aggressive timers "hello-interval 1" and "dead-interval 4"
CSCvq50846	ip verify source mac-check prevents device tracking from getting arp probe reply
CSCvq55940	%BIT-4-OUTOFRANGE: bit 4095 is not in the expected range of 1 to 4093
CSCvq66802	igmp query with src ip 0.0.0.0 is not ignored
CSCvq68337	Cat3k/9k does not forward packet when active route down
CSCvq72472	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvq72713	Cat3k/Cat9k can't forwarding traffic follow the rule of EIGRP unequal cost load-balancing
CSCvq75887	intermediate hop with SVI in PIM domain is not forwarding multicast traffic
CSCvq94738	The COPP configuration back to the default After rebooting the device
CSCvr03905	Memory Leak on FED due to IPv6 Source Guard
CSCvr04551	Multicast stream flickers on igmp join/leave
CSCvr08351	Rework CSCvq82313: Catalyst 9300 sif_mgr process crash.
CSCvr20522	Cat3k/9k BOOTREPLY dropped when DHCP snooping is enabled
CSCvr23358	Switches are adding Device SGT to proxy generated IGMP leave messages while keeping End host src IP
CSCvr30559	Switch may experience a kernel panic due to invalid skb
CSCvr46931	ports remain down/down object-manager (fed-ots-mo thread is stuck)
CSCvr48249	High memory utilization under fman_fp_image
CSCvr59959	Cat3k/9k Flow-based SPAN(FSPAN) can only work in one direction when mutilple session configured
CSCvr88090	Cat3k/9k crash on running show platform software fed switch 1 fss abstraction

Identifier	Description
CSCvr95643	Silent loss and TCP Re-transmissions seen with certain host pcs connected to c9300-48UXM
CSCvr98281	After valid ip conflict, SVI admin down responds to GARP
CSCvr98368	CAT9K intermittently not responding to SNMP
CSCvs22885	C9300-NM-8X - SFP-10G module gbic-invalid err-disable
CSCvs50868	Fed memory leak in 16.9.X related to netflow

Resolved Caveats in Cisco IOS XE Fuji 16.9.4

Caveat ID Number	Description
CSCvj15473	Linux IOSD crash with sh vtp counters cmd
CSCvj16691	port LED may turn to amber
CSCvj28615	Enhancement to change pethMainPowerUsageOnNotification default threshold from 0
CSCvj84601	Called-Station-Id attribute not included in Radius Access-Request
CSCvk44346	Power high priority not observed in Strict mode on 9300
CSCvk60809	Wrong Time-Stamp is saved in pcap.
CSCvm80443	IOSd memory leak within DSMIB Server within xqos_malloc_wrapper
CSCvm91107	standby reloads and crashed @fnf_ios_config_dist_validate_sel_process_add
CSCvm91642	MACsec SAP 128 Bits doesn't work with network-essentials license
CSCvn30230	Catalyst 3k/9k: Slow memory leak in linux_iosd-imag
CSCvn57892	High Memory utilization due to Wireless Manager IOSD process
CSCvn69629	ND packets received in remote vtep SISF table - EVPN part
CSCvn99482	IPv6 traffic is stopped on interface when more than 3 invalid ARPs are detected
CSCvn99621	hw-switch logging onboard message may be disappeared after reload
CSCvo05751	Changes for sending vlan attrs in access request
CSCvo21122	Memory leak at hman process
CSCvo40004	C9300-48P | 100/Full interfaces not coming up right after bootup
CSCvo42353	SDA-Cat9k-External border creating incorrect CEF/map-cache entry due to multicast

Caveat ID Number	Description
CSCvo49876	SISF not honoring 1 IPv4-to-MAC rule when DHCP ACK comes from a different VLAN (via Relay)
CSCvo57768	NetFlow issue 3850 switch not sending TCP flags
CSCvo60400	errdisable detect cause bpduguard shutdown vlan continues to forward BPDUs
CSCvo61570	spanning-tree uplinkfast max-update-rate's value is abnormal
CSCvo65974	QinQ tunnels causing L2 loop in specific topology of Cat3850
CSCvo66246	Enabling SPAN source of VLAN 1 affects LACP operations
CSCvo71264	Cat3k / Cat9k Gateway routes DHCP offer incorrectly after DHCP snooping
CSCvo73205	Identity policy won't update after config changes.
CSCvo73897	[SDA] [PI changes] No audio during first few seconds of voice call between 2 Fabric Edge
CSCvo74750	High Temperature returned for Catalyst switches when the inlet temperature is negative
CSCvo75559	Cat9300 | First packet not forwarded when (S,G) needs to be built
CSCvo78538	Counters in the "show interface" command are not increasing
CSCvo85422	Directly connected IPv4/IPv6 hosts not programmed in HW - %FMFP-3-OBJ_DWNLD_TO_DP_FAILED
CSCvp00026	[SDA] [PD changes] No audio during first few seconds of voice call between 2 Fabric Edge
CSCvp03816	ENH Hex dump constantly logging when registering access point using DNAC
CSCvp09091	When sourcing Radius from loopback in VRF, auth right out of boot up might fail
CSCvp12187	Standby switch crash due to memory leak due to Switch Integrated Security feature
CSCvp13114	Cat9400 incoming packet from PVLAN access port is not forwarded out on etherchannel interface
CSCvp26792	Cat9k control plane impacted when > 1Gbps multicast passes through and no entry in IGMP snooping
CSCvp30239	memory leak when there are constant changes in REP ring
CSCvp30629	Cat9300: Lisp site entry count mismatch in external dual border on reload
CSCvp33294	Cat9k || Asic 0 Core 0 buffer stuck, rwePbcStall seen
CSCvp37754	9300 non mgig - Half-Pair Ethernet Cables do not auto-negotiate to 100 Full with Certain IP Phones
CSCvp49518	DHCP SNOOPING DATABASE IS NOT REFRESHED AFTER RELOAD

Caveat ID Number	Description
CSCvp54779	[SDA] 1st ARP Reply is dropped at remote Fabric Edge
CSCvp65173	SDA: DHCP offer being dropped on BN with L2 and L3 Handoff configured
CSCvp72220	crash at sisf_show_counters after entering show device-tracking counters command
CSCvp75221	Modules shows faulty status when specific MAC ACL is applied on interfaces
CSCvp81190	%FED_QOS_ERRMSG-3-TABLEMAP_INGRESS_HW_ERROR was generated after setting policy-map with table-map
CSCvp85601	STP TCN is generated on etherchannel port during a switchover in a 3850 stack
CSCvp86983	Connectivity over AC tunnel broken due to tunnel deletion from FMAN FP but remains FMAN FP
CSCvp89755	VPN label is wrongly derived as explicit-null in Cat9k for L3 VPN traffic
CSCvp90279	Catalyst switches is sending ADV and REP DHCPv6 packets to SISF when source udp port is not 547
CSCvq01185	%SNMP-3-RESPONSE_DELAYED: and timeout when polling entSensorValueEntry on 16.9.3
CSCvq25360	PD's not getting PoE on multiple interfaces in 3850 stack
CSCvq30316	[SDA] 1st ARP fix for CSCvp00026 is eventually failing after longevity
CSCvq30460	SYS-2-BADSHARE: Bad refcount in datagram_done - messages seen during system churn
CSCvq40137	Mac address not being learnt when "auth port-control auto" command is present
CSCvq55779	FIVE GIG INTERFACE NOT SHOWING IN CLI WHILE CONFIGURING IP IGMP SNOOPING

Resolved Caveats in Cisco IOS XE Fuji 16.9.3

Identifier	Description
CSCuw36080	SNMP with Extended ACL
CSCvd72166	Uneven available power distribution when using power sharing
CSCvh77984	Router shows "Flash disk quota exceeded" during the reload, but it still has 60% of free memory left
CSCvi48988	SNMP timeout when querying entSensorValueEntry
CSCvj79694	sgt-map gets cleared for some of the end points for unknown reason
CSCvk45142	Crash with smd fault on rp_0_0

Identifier	Description
CSCvm07353	Router may crash when a SSH session is closed after configure TACACS
CSCvm36333	MAC address programming issue
CSCvm47335	IOSd: large amount of bursty IPC traffic sometime can cause high CPU utilization in fastpath
CSCvm77197	C9300 : %IOSXE-2-PLATFORM: Switch 1 R0/0: kernel: EXT2-fs (sda1): error:
CSCvm86478	RMON statistics and RMON MIB absent in cat9K
CSCvm87134	Cat9K stackwise-virtual- Smart license registration status is lost after 2 to 3 multiple reloads/SSO
CSCvm94788	Device reloads when applying #client <IP> vrf Mgmt-vrf server-key 062B0C09586D590B5656390E15
CSCvn02171	HOLE is not created when acl default passthrough configured
CSCvn08672	DHCP packets cause unknown protocol drops
CSCvn30138	Crash with show service-insertion service-context command in AppNav Cluster
CSCvn30950	16.10.1: c9300 stack could run into a state where all member switch are removed until reboot
CSCvn31653	Missing/incorrect FED entries for IGMP Snooping on Cat9300/Cat3850/Cat3650
CSCvn36494	WCCP redirection to proxy server breaks in certain scenarios.
CSCvn38590	CTS policies download fails with Missing/Incomplete ACEs error
CSCvn40414	PSU shown as Disabled when there is not input power cables.
CSCvn46334	show inventory does not list the Stack Ports / Stack cables after reload
CSCvn46925	IPv6 multicast packet ff02::1:2 /DHCPv6 solicitation with L2 flooding impacts BFD/ISIS control pkts
CSCvn58515	Ac Tunnel in "pending-issue-update" state in FMAN FP
CSCvn60419	SDA:ICMPv6 neighbor Advertisement loop with L2 flooding feature enabled
CSCvn71041	TACACS group server is not seen, when "transport-map type console test" is configured.
CSCvn72973	Device is getting crashed on the "cts role-based enforcement"
CSCvn97961	9300 Mgig port 5 - Interface don't come UP and Can't read port related CLI
CSCvo00968	Radius attr 32 NAS-IDENTIFIIER not sending the FQDN
CSCvo03530	C9500- Remote side link stays up on reload with GLC-T/QSA.

Identifier	Description
CSCvo15594	MATM programming issue for remote client 9300
CSCvo17778	Cat9k not updating checksum after DSCP change
CSCvo32446	High CPU Due To Looped Packet and/or Unicast DHCP ACK Dropped
CSCvo33983	Mcast traffic loss seen looks due to missing fed entries during IGMP/MLD snooping.

Resolved Caveats in Cisco IOS XE Fuji 16.9.2

Identifier	Description
CSCvg81784	Converting a layer 2 port-channel to L3 causes some Protocols to break
CSCvi49725	C9300: Group of 4 ports stop forwarding traffic
CSCvi90160	Incremental Rx bytes Counter increase while ports inactive
CSCvj16271	Addressing memory leaks in IPC error handling cases in LED, RPS, VMARGIN, USB, THERMAL
CSCvj31854	REP Node reload causes unicast traffic drops on a neighbor switch
CSCvj66609	DHCP offer received from SVI sent back to the same SVI when DHCP Snooping is enabled
CSCvj74923	Client does not get the reserved IP Address for the interface on Port based DHCP configuration.
CSCvj75719	System returning incorrect portchannel MIB value (IEEE8023-LAG-MIB)
CSCvk02591	When 10000 speed is configured on C9300-NM-4M uplink port , sh int status displays as 100
CSCvk08304	Slowness for x11perf with MGig port on 9300
CSCvk16813	DHCP client traffic dropped with DHCP snooping and port-channel or cross stack uplinks.
CSCvk47653	Stack member crash during LACP port aggregation
CSCvk49306	The active switch is not detecting USB device/usbflash0 when inserting a USB drive
CSCvk53444	Packets with Fragment Offset not forwarded with DHCP Snooping Enabled
CSCvm07921	OOB TX path excessive congestion cause software to force crash a switch
CSCvm51584	Copper 25G SFPs not defaulting to autoneg

Resolved Caveats in Cisco IOS XE Fuji 16.9.1

Identifier	Description
CSCvg53159	%SNMP-3-RESPONSE_DELAYED: processing GetNext of cafSessionEntry.2 seen on catalyst switch
CSCvg58417	Unwanted messages seen during removal of USB 3.0 SSD
CSCvg67012	Deprecate the option of member flash# in upgrade/downgrade CLI for software install
CSCvg95580	interface speed config went lost after same FRU OIR with "write mem"
CSCvh28104	QSFP-H40G-CU5M 40g not showing as up on peer
CSCvh49334	Cat9300 stops forwarding multicast - L3M Failed to allocate REP RI
CSCvh63530	MPLS traffic drops with ECMP loadbalance towards core. All cat9ks
CSCvh84345	IOS CLI "show platform software fed switch active punt cause summary" may display negative counts
CSCvh87131	TRACEBACK: OID cefcModuleEntry crashes the box
CSCvh96261	EXP based Queuing on cat9k platforms
CSCvi01682	DOM data not available on SFP with QSA adapter when port is shut down
CSCvi08459	set different words for username and password, but username shown the same as password
CSCvi26179	Cat9k crash while accessing OBFL
CSCvi33020	QSFP-40G-SR4 (4X10G mode) in err_disable state on C9300 (2x40G uplink)
CSCvi38191	Memory leak in lman process due to "ld_license_ext.dat" build-up.
CSCvi39202	DHCP fails when DHCP snooping trust is enabled on uplink etherchannel
CSCvi48995	On mGig SKU (downlink ports) - Link down with forced speed100/full duplex on both ends
CSCvi75086	Rapid TDL memory leak in SMD process leads to crash of active switch in stack for ipv6 clients
CSCvi75488	Ping from client fails with enforcement enabled on known mappings
CSCvj69569	"sh auth sess sw st" broken and session monitoring sessions coming in sh auth sess in legacy mode.

Troubleshooting

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

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

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

Related Documentation

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

All support documentation for Cisco Catalyst 9300 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html

Cisco Validated Designs documents at this URL: https://www.cisco.com/go/designzone

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.