Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Fuji 16.9.x

First Published: 2018-07-18

Last Modified: 2021-09-01

Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Fuji 16.9.x

Introduction

Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance are Cisco's lead, fixed core and aggregation enterprise switching platforms. They have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

They deliver complete convergence in terms of ASIC architecture with Unified Access Data Plane (UADP) 2.0 on Cisco Catalyst 9500 Series Switches and UADP 3.0 on Cisco Catalyst 9500 Series Switches - High Performance. 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 With the introduction of the High Performance models in the series, there may be differences in the supported and unsupported features, limitations, and caveats that apply to the Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance models. Throughout this release note document, any such differences are expressly called out. If they are not, the information applies to all models in the series.

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 49.

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 49.

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 49.

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 49.

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 49.

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 49.

Whats New in Cisco IOS XE Fuji 16.9.2

Software Features in Cisco IOS XE Fuji 16.9.2

Software Features Introduced on Cisco Catalyst 9500 Series Switches

(C9500-12Q, C9500-16X, C9500-24Q, C9500-40X)

Feature Name	Description, License Level Information, Documentation Link
In Service Software Upgrade (ISSU)	A process that allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades. **Note** Starting with this release, this feature is supported on the following models of the Cisco Catalyst 9500 Series Switches, with the Cisco Stackwise Virtual feature: • C9500-24Q • C9500-12Q • C9500-40X • C9500-16X (Network Advantage)

Whats New in Cisco IOS XE Fuji 16.9.1

Hardware Features in Cisco IOS XE Fuji 16.9.1

- Hardware Features Introduced on Cisco Catalyst 9500 Series Switches
- Hardware Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance

Hardware Features Introduced on Cisco Catalyst 9500 Series Switches

Feature Name	Description
Cisco 40GBASE QSFP Module (4x10G mode qualification)	• Supported transceiver module number—QSFP-40G-CSR4 • Compatible switch models—C9500-12Q and C9500-24Q • Compatible networl 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 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 hot-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. See Cisco Catalyst 9500 Series Switches Hardware Installation Guide → Installing Field Replaceable Units
A higher number of switch ports supported for QSFP-4X10G-LR-S	The QSFP-4X10G-LR-S module can now be installed on port numbers 1 through 12 of the C9500-12Q and C9500-24Q switch models. (Only port numbers 1 through 4 were supported in an earlier release).

Hardware Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance

Feature Name	Description
Cisco 1000BASE-T SFP Transceiver Module	• Supported transceiver module product numbers—GLC-T, GLC-TE • Compatible switch models—C9500-48Y4C and C9500-24Y4C For information about the modules, see Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet. For information about device compatibility, see the Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix.
Cisco 25GBASE SFP28 Transceiver Module—Cisco SFP-10/25G-CSR-S	• Supported transceiver module product numbers—Cisco SFP-10/25G-CSR-S • Compatible switch models—C9500-48Y4C and C9500-24Y4C 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 QSFP 40-Gigabit Ethernet to SFP+ 10G Adapter Module (Cisco QSA Module)—CVR-QSFP-SFP10G	• Supported transceiver module product number—CVR-QSFP-SFP10G This module offers 10 Gigabit Ethernet and 1 Gigabit Ethernet connectivity for Quad Small Form-Factor Pluggable (QSFP)-only platforms by converting a QSFP port into an SFP or SFP+ port. • Compatible switch models—C9500-48Y4C and C9500-24Y4C uplink ports **Note** The module can now be installed on uplink ports. This was was not supported when support for the module was first introduced in an earlier release. For information about the adapter, see the Cisco QSFP to SFP or SFP+ Adapter Module Data Sheet. For information about device compatibility, see the Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix.
M.2 Serial Advanced Technology Attachment (SATA) Storage	Provides extra storage to host applications and to capture packet trace logs. M.2 SATA also supports Self-Monitoring, Analysis and Reporting Technology System (S.M.A.R.T.) attributes. You can monitor the health of SATA device through the S.M.A.R.T tools integrated in the Cisco IOS XE Fuji 16.9.1 image.

Software Features in Cisco IOS XE Fuji 16.9.1

Software Features Introduced on All Models

Feature Name	Description, License Level Information, Documentation Link
Hot Patching Support	Allows Software Maintenance Upgrade (SMU) to happen immediately after activation, without reloading the system. SMU is a package that can be installed on a system to provide a fix or a security resolution to a released image. The package is provided on a per release and per component basis. See System Management → Software Maintenance Upgrade . (Network Advantage for CLI and DNA Advantage for DNAC)
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)
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)

Feature Name	Description, License Level Information, Documentation Link
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)
Network Address Translation (NAT) with scale enhancement	When configuring SDM templates for NAT usage, the maximum number of sessions that can be translated and forwarded in the hardware, in an ideal setting, is optimised to 14,000. See IP → Configuring Network Address Translation . (DNA 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, License Level Information, Documentation Link
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.
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 45 section in this release note document. A license level is not applicable.

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.

Software Features Introduced on Cisco Catalyst 9500 Series Switches

(C9500-12Q, C9500-16X, C9500-24Q, C9500-40X)

Feature Name	Description, License Level Information, Documentation Link
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)

Feature Name	Description, License Level Information, Documentation Link
Cisco StackWise Virtual – Enhancement relating to supported ports	Cisco StackWise Virtual was supported on a restricted number of ports on the Cisco Catalyst 9500 Series Switches. Starting from this release, this restriction has been removed and the feature can be configured on all the fixed ports of these models: • C9500-24Q • C9500-12Q • C9500-40X • C9500-16X **Note** You still cannot configure Cisco StackWise Virtual links on the uplink (network) modules (C9500-NM-8X and C9500-NM-2Q). See High Availability → Configuring Cisco StackWise Virtual Also see these sections in this release note document for other important information about the feature: • Important Notes → Cisco StackWise Virtual - Supported and Unsupported Features • Limitations and Restrictions → Cisco StackWise Virtual
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 the hardware functionality. See System Management → Configuring Online Diagnostics . (Network Essentials and Network Advantage)

Feature Name	Description, License Level Information, Documentation Link
Graceful Insertion and Removal (GIR) enhancements	The feature uses a maintenance mode to isolate the switch from the network in order to perform debugging, or an upgrade. When you place the switch in maintenance mode, supported protocols are isolated, and Layer 2 interfaces are shut down. When normal mode is restored, the supported protocols and ports are brought back up. These enhancements have been added to the GIR feature in this release: • 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 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 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 High Availability → Configuring Graceful Insertion and Removal . (Network Advantage)

Feature Name	Description, License Level Information, Documentation Link
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)
REP downlink support	Allows REP configuration on downlink ports. See Layer 2 → Configuring Resilient Ethernet Protocol . (Network Essentials and Network Advantage)
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)

Software Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance

(C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C)

Feature Name	Description, License Level Information, Documentation Link
Boot Integrity Visibility	Allows Cisco's platform identity and software integrity information to be visible and actionable. Platform identity provides the platform's manufacturing installed identity, and software integrity exposes boot integrity measurements that can be used to assess whether the platform has booted trusted code. See System Management → Boot Integrity Visibility . (Network Essentials and Network Advantage)

Feature Name	Description, License Level Information, Documentation Link
Disabling MAC Address Learning on VLAN	The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. By default, MAC address learning is enabled on all interfaces and VLANs on the router. You can control MAC address learning on VLAN to manage the available MAC address table space by controlling which VLANs can learn the MAC addresses. Before you disable MAC address learning, be sure that you are familiar with the network topology and the router system configuration. Disabling MAC address learning on aVLAN could cause flooding in the network. See System Management → Administering the Device . (Network Essentials and Network Advantage)
Encapsulated Remote Switched Port Analyzer (ERSPAN)	ERSPAN enables you to monitor traffic on ports or VLANs and to send monitored traffic to destination ports. Starting with this release, the **header-type 3**, **destination**, **ip dscp**, and **vrf** ERSPAN monitor source session configuration mode commands, and **sgt** keyword are introduced. See Network Management → Configuring ERSPAN . (DNA Advantage)
Fast Unidirectional Link Detection (UDLD)	Enables subsecond UDLD. The UDLD protocol helps monitor a physical connection (such as monitoring wrong cabling) to detect unidirectional links to avoid spanning-tree topology loops or silent drop traffic. See Layer 2 → Configuring UniDirectional Link Detection . (Network Essentials and Network Advantage)
IPv6 Support for SGT and SGACL	Facilitates dynamic learning of mappings between IP addresses and Security Group Tags (SGTs) for IPv6 addresses. The SGT is then used to derive the Security Group Access Control List (SGACL). See Cisco TrustSec → IPv6 Support for SGT and SGACL . (Network Advantage)

Feature Name	Description, License Level Information, Documentation Link
Multiprotocol Label Switching • Ethernet over MPLS (EoMPLS) • Virtual Private LAN Services (VPLS) • external BGP (eBGP) and internal BGP (iBGP)	The following MPLS features are introduced in this release: • EoMPLS—One of the Any Transport over MPLS (AToM) transport types. EoMPLS provides a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core. It encapsulates Ethernet protocol data units (PDUs) inside MPLS packets and uses label stacking to forward them across the MPLS network. • VPLS—A class of VPN that supports the connection of multiple sites in a single bridged domain over a managed IP/MPLS network. VPLS uses the provider core to join multiple attachment circuits together, to simulate a virtual bridge that connects the multiple attachment circuits together. • eBGP and iBGP—Enables you to configure multipath load balancing with both eBGP and iBGP paths in Border Gateway Protocol (BGP) networks that are configured to use MPLS VPNs. The feature provides improved load balancing deployment and service offering capabilities and is useful for multi-homed autonomous systems and Provider Edge (PE) routers that import both eBGP and iBGP paths from multihomed and stub networks. See Multiprotocol Label Switching (MPLS) . (Network Advantage)
SGT Name Export in NetFlow	Allows Flexible NetFlow to export Cisco TrustSec environmental data tables that map SGTs to Security Group Names. See Cisco TrustSec → Flexible NetFlow Export of Cisco TrustSec Fields . (DNA Essentials and DNA Advantage)
Top-N Reports	Enable you to collect and analyze data for each physical port on a switch. When Top-N reports start, they obtain statistics from the appropriate hardware counters and then go into sleep mode for a user-specified interval. When the interval ends, the reports obtain current statistics from the same hardware counters, compare current statistics with the earlier statistics, and store the difference. See Network Management → Top-N Reports . (Network Essentials and Network Advantage)

Important Notes

Cisco StackWise Virtual - Supported and Unsupported Features

(applies only to C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models)

When you enable Cisco StackWise Virtual on the device

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

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

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

Unsupported Features—All Models

- Bluetooth
- Bidirectional Protocol Independent Multicast (Bidir-PIM)
- IPsec VPN
- Performance Monitoring (PerfMon)
- Virtual Routing and Forwarding (VRF)-Aware web authentication

Unsupported Features—Cisco Catalyst 9500 Series Switches

- Border Gateway Protocol (BGP) Additional Paths
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Flexible NetFlow—NetFlow v5 Export Protocol, 4-byte (32-bit) AS Number Support, TrustSec NetFlow IPv4 Security Group Access Control List (SGACL) Deny and Drop Export
- Gateway Load Balancing Protocol (GLBP)
- Lawful Intercept (LI)
- Network-Powered Lighting (including COAP Proxy Server, 2-event Classification, Perpetual POE, Fast PoE)

- PIM Bidirectional Forwarding Detection (PIM BFD), PIM Snooping.
- Quality of Service—Classification (Layer 3 Packet Length, Time-to-Live (TTL)), per queue policer support, sharped profile enablement for egress per port queues, L2 Miss, Ingress Packet FIFO (IPF)
- Unicast over Point to Multipoint (P2MP) Generic Routing Encapsulation (GRE), Multicast over P2MP GRE.
- VLAN Translation—One-to-One Mapping

Unsupported Features—Cisco Catalyst 9500 Series Switches - High Performance

- Cisco Application Visibility and Control (AVC)
- Cisco Stackwise Virtual
- Graceful Insertion and Removal (GIR)
- In Service Software Upgrade (ISSU)
- MPLS Label Distribution Protocol (MPLS LDP) VRF-Aware Static Labels
- Next Generation Network-Based Application Recognition (NBAR) and Next Generation NBAR (NBAR2)
- Nonstop Forwarding (NSF), Enhanced Interior Gateway Routing Protocol (EIGRP) NSF and Open Shortest Path First (OSPF) NSF, NSF support for IPv6, NSF Awareness (BGP, EIGRP, OSPF))
- QoS Options on GRE Tunnel Interfaces
- Stateful Switchover (SSO)

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.

When you search for the list of features by platform select

- CAT9500—to see all the features supported on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models
- CAT9500 HIGH PERFORMANCE (32C; 32QC; 48Y4C; 24Y4C)—to see all the features supported on the C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C models

Accessing Hidden Commands

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

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

Starting with Cisco IOS XE Fuji 16.8.1a, hidden commands are available under:

- Category 1—Hidden commands in privileged or User EXEC mode. Begin by entering the **service internal** command to access these commands.

- Category 2—Hidden commands in one of the configuration modes (global, interface and so on). These commands do not require the **service internal** command.

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

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

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

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

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

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

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

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

Supported Hardware

Cisco Catalyst 9500 Series Switches—Model Numbers

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

Base PIDs are the model numbers of the switch.

Bundled PIDs indicate the orderable part numbers for base PIDs that are bundled with a particular network module. Entering the **show version**, **show module**, or **show inventory** commands on such a switch (bundled PID), displays its base PID.

Table 1: Cisco Catalyst 9500 Series Switches

Switch Model	Default License Level[1]	Description
Base PIDs		
C9500-12Q-E	Network Essentials	12 40-Gigabit Ethernet QSFP+ ports and two power supply slots
C9500-12Q-A	Network Advantage	
C9500-16X-E	Network Essentials	16 1/10-Gigabit Ethernet SFP/SFP+ ports and two power supply slots
C9500-16X-A	Network Advantage	

Switch Model	Default License Level[1]	Description
C9500-24Q-E	Network Essentials	24-Port 40-Gigabit Ethernet QSFP+ ports and two power supply slots
C9500-24Q-A	Network Advantage	
C9500-40X-E	Network Essentials	40 1/10-Gigabit Ethernet SFP/SFP+ ports and two power supply slots
C9500-40X-A	Network Advantage	
Bundled PIDs		
C9500-16X-2Q-E	Network Essentials	16 10-Gigabit Ethernet SFP+ port switch and a 2-Port 40-Gigabit Ethernet (QSFP) network module on uplink ports
C9500-16X-2Q-A	Network Advantage	
C9500-24X-E	Network Essentials	16 10-Gigabit Ethernet SFP+ port switch and an 8-Port 10-Gigabit Ethernet (SFP) network module on uplink ports
C9500-24X-A	Network Advantage	
C9500-40X-2Q-E	Network Essentials	40 10-Gigabit Ethernet SFP+ port switch and a 2-Port 40-Gigabit Ethernet (QSFP) network module on uplink ports
C9500-40X-2Q-A	Network Advantage	
C9500-48X-E	Network Essentials	40 10-Gigabit Ethernet SFP+ port switch and an 8-Port 10-Gigabit Ethernet (SFP) network module on uplink ports
C9500-48X-A	Network Advantage	

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

Table 2: Cisco Catalyst 9500 Series Switches-High Performance

Switch Model	Default License Level[2]	Description
C9500-24Y4C-E	Network Essentials	24 SFP28 ports that support 1/10/25-GigabitEthernet connectivity, four QSFP uplink ports that support 100/40-GigabitEthernet connectivity; two power supply slots.
C9500-24Y4C-A	Network Advantage	
C9500-32C-E	Network Essentials	32 QSFP28 ports that support 40/100 GigabitEthernet connectivity; two power supply slots.
C9500-32C-A	Network Advantage	
C9500-32QC-E	Network Essentials	32 QSFP28 ports, where you can have 24 ports that support 40-GigabitEthernet connectivity and 4 ports that support 100-GigabitEthernet connectivity, OR 32 ports that support 40-GigabitEthernet connectivity, OR 16 ports that support 100-GigabitEthernet connectivity; two power supply slots.
C9500-32QC-A	Network Advantage	

Switch Model	Default License Level[2]	Description
C9500-48Y4C-E	Network Essentials	48 SFP28 ports that support 1/10/25-GigabitEthernet connectivity; four QSFP uplink ports that supports up to 100/40-GigabitEthernet connectivity; two power supply slots.
C9500-48Y4C-A	Network Advantage	

[2] 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 optional network modules for uplink ports available with some configurations .

Network Module	Description
C9500-NM-8X	Cisco Catalyst 9500 Series Network Module 8-port 1/10 Gigabit Ethernet with SFP/SFP+ Note the supported switch models (Base PIDs): • C9500-40X • C9500-16X
C9500-NM-2Q	Cisco Catalyst 9500 Series Network Module 2-port 40 Gigabit Ethernet with QSFP+ Note the supported switch models (Base PIDs): • C9500-40X • C9500-16X

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 9500 and 9500-High Performance	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**.
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**.

Catalyst 9500 and 9500-High Performance	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
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**
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[3]	512 MB[4]	256	1280 x 800 or higher	Small

[3] We recommend 1 GHz
[4] 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.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.08.SPA.bin
Cisco IOS XE Fuji 16.9.7	CAT9K_IOSXE	cat9k_iosxe.16.09.07.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.07.SPA.bin
Cisco IOS XE Fuji 16.9.6	CAT9K_IOSXE	cat9k_iosxe.16.09.06.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.06.SPA.bin

Release	Image Type	File Name
Cisco IOS XE Fuji 16.9.5	CAT9K_IOSXE	cat9k_iosxe.16.09.05.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.05.SPA.bin
Cisco IOS XE Fuji 16.9.4	CAT9K_IOSXE	cat9k_iosxe.16.09.04.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.04.SPA.bin
Cisco IOS XE Fuji 16.9.3	CAT9K_IOSXE	cat9k_iosxe.16.09.03.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.03.SPA.bin
Cisco IOS XE Fuji 16.9.2	CAT9K_IOSXE	cat9k_iosxe.16.09.02.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.09.02.SPA.bin
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.bin

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.	On Cisco Catalyst 9500 Series Switches, 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)`
	On Cisco Catalyst 9500 Series Switches - High Performance, 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 or 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 Jul 5 18:03:28 Universal 2018 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`waiting for upgrades to complete...`

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 **Note** **This table of commands is not supported on Cisco Catalyst 9500 Series Switches - High Performance.**	
`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 with In Service Software Upgrade (ISSU) with Cisco StackWise Virtual

Follow these instructions to perform ISSU upgrade from Cisco IOS XE Fuji 16.9.2 to Cisco IOS XE Fuji 16.9.3, in install mode with Cisco StackWise Virtual. Step 2 to Step 7 are optional and should be used when you are running prerequisite checks before performing ISSU.

Before you begin

In Service Software Upgrade (ISSU) from Cisco IOS XE Fuji 16.9.2 to Cisco IOS XE Fuji 16.9.3 with Cisco StackWise Virtual requires installation of Software Maintenance Upgrade (SMU) packages. Install the following SMU packages before performing ISSU.

Release	File Name (Hot Patch)
Cisco IOS XE Fuji 16.9.2	cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin

Note Downgrade with ISSU is not supported. To downgrade, follow the instructions in the Downgrading in Install Mode, on page 39 section.

For more information about ISSU release support and recommended releases, see Technical References → In-Service Software Upgrade (ISSU).

Procedure

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Switch# enable
```

Step 2 **show version | in INSTALL** or **show version | in System image**

Use **show version | in INSTALL** command to check the boot mode. ISSU is supported only in install mode. You cannot perform ISSU if the switch is booted in bundle mode.

```
Switch# show version | in INSTALL
Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*    1 12    C9500-12Q          16.9.1            CAT9K_IOSXE           INSTALL
     2 12    C9500-12Q          16.9.1            CAT9K_IOSXE           INSTALL
```

Step 3 **dir flash: | in free**

Use this command to check if there is sufficient available memory on flash. Ensure that you have at least 1GB of space in flash to expand a new image.

```
Switch# dir flash: | in free
11353194496 bytes total (8565174272 bytes free)
```

Step 4 **show redundancy**

Use this command to check if the switch is in SSO mode.

```
Switch# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 4 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up
<output truncated>
```

Step 5 **show boot system**

Use this command to verify that the manual boot variable is set to **no**.

```
Switch# show boot system
Current Boot Variables:
BOOT variable = flash:packages.conf;
MANUAL_BOOT variable = no

Boot Variables on next reload:
BOOT variable = flash:packages.conf;
MANUAL_BOOT variable = no
Enable Break = no
Boot Mode = DEVICE
iPXE Timeout = 0
```

If the manual boot variable is set to **yes**, use the **no boot manual** command in global configuration mode to set the switch for autoboot.

Step 6 **show issu state** [*detail*]

Use this command to verify that no other ISSU process is in progress.

```
Switch# show issu state detail
--- Starting local lock acquisition on chassis 2 ---
Finished local lock acquisition on chassis 2

No ISSU operation is in progress

Switch#
```

Step 7 **show install summary**

Use this command to verify that the state of the image is *Activated & Committed*. Clear the install state if the state is not *Activated & Committed*.

```
Switch# show install summary
[ Switch 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    16.9.2.0.2433
```

Step 8 **install add file activate commit**

Use the commands below to install the maintenance update packages. You can point to the source image on your TFTP server or in flash if you have it copied to flash.

```
Switch# install add file tftp:cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin activate commit
```

To verify if the SMU packages are installed properly, use **show install summary** command.

```
Switch# show install summary
[ Switch 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    flash:cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin
IMG   C    16.9.2.0.2433
```

The following sample output displays installation of CSCvo12166 SMU, by using the **install add file tftp:cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin activate commit** command.

```
Switch# install add file tftp:cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin activate commit
install_add_activate_commit: START Thu Mar 21 05:58:45 UTC 2019
Downloading file tftp://172.27.18.5//cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin
Finished downloading file tftp://172.27.18.5//cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin
to flash:cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin
install_add_activate_commit: Adding SMU

--- Starting initial file syncing ---

*Mar 21 05:58:46.446: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine: Started
 install one-shot tftp://172.27.18.5//cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin[1]: Copying
 flash:cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin from switch 1 to switch 2
[2]: Finished copying to switch 2
Info: Finished copying flash:cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin to the selected
```

```
switch(es)
Finished initial file syncing

Executing pre scripts....
Executing pre sripts done.
--- Starting SMU Add operation ---
Performing SMU_ADD on all members
  [1] SMU_ADD package(s) on switch 1
  [1] Finished SMU_ADD on switch 1
  [2] SMU_ADD package(s) on switch 2
  [2] Finished SMU_ADD on switch 2
Checking status of SMU_ADD on [1 2]
SMU_ADD: Passed on [1 2]
Finished SMU Add operation

install_add_activate_commit: Activating SMU
Executing pre scripts....
Executing pre sripts done.

--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
  [1] SMU_ACTIVATE package(s) on switch 1
  [1] Finished SMU_ACTIVATE on switch 1
  [2] SMU_ACTIVATE package(s) on switch 2
  [2] Finished SMU_ACTIVATE on switch 2
Checking status of SMU_ACTIVATE on [1 2]
SMU_ACTIVATE: Passed on [1 2]
Finished SMU Activate operation

SUCCESS: install_add_activate_commit /flash/cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin Thu
 Mar 21 05:59:06 UTC 2019

Switch#
*Mar 21 05:59:06.399: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_engine:
Completed install one-shot SMU flash:cat9k_iosxe.16.09.02.CSCvo12166.SPA.smu.bin
Switch#
```

Step 9 install add file activate issu commit

Use this command to automate the sequence of all the upgrade procedures, including downloading the images to both the switches, expanding the images into packages, and upgrading each switch as per the procedures.

```
Switch# install add file tftp:cat9k_iosxe.16.09.03.SPA.bin activate issu commit
```

The following sample output displays installation of Cisco IOS XE Fuji 16.9.3 software image with ISSU procedure.

```
Switch# install add file tftp:cat9k_iosxe.16.09.03.SPA.bin activate issu commit
install_add_activate_commit: START Thu Mar 21 06:16:32 UTC 2019
Downloading file tftp://172.27.18.5//cat9k_iosxe.16.09.03.SPA.bin

*Mar 21 06:16:34.064: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine: Started
 install one-shot ISSU tftp://172.27.18.5//cat9k_iosxe.16.09.03.SPA.binFinished downloading
 file tftp://172.27.18.5//cat9k_iosxe.16.09.03.SPA.bin to flash:cat9k_iosxe.16.09.03.SPA.bin
install_add_activate_commit: Adding ISSU

--- Starting initial file syncing ---
[1]: Copying flash:cat9k_iosxe.16.09.03.SPA.bin from switch 1 to switch 2
[2]: Finished copying to switch 2
Info: Finished copying flash:cat9k_iosxe.16.09.03.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
  [2] Add package(s) on switch 2
  [2] Finished Add on switch 2
Checking status of Add on [1 2]
Add: Passed on [1 2]
Finished Add

install_add_activate_commit: Activating ISSU

NOTE: Going to start Oneshot ISSU install process

STAGE 0: Initial System Level Sanity Check before starting ISSU
================================================
--- Verifying install_issu supported ---
--- Verifying standby is in Standby Hot state ---
--- Verifying booted from the valid media ---
--- Verifying AutoBoot mode is enabled ---
Finished Initial System Level Sanity Check


STAGE 1: Installing software on Standby
================================================
--- Starting install_remote ---
Performing install_remote on Chassis remote
[2] install_remote package(s) on switch 2
[2] Finished install_remote on switch 2
install_remote: Passed on [2]
Finished install_remote


STAGE 2: Restarting Standby
================================================
--- Starting standby reload ---
Finished standby reload

--- Starting wait for Standby to reach terminal redundancy state ---

*Mar 21 06:24:16.426: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Mar 21 06:24:16.426: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Mar 21 06:24:16.466: %HMANRP-5-CHASSIS_DOWN_EVENT: Chassis 2 gone DOWN!
*Mar 21 06:24:16.497: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_NOT_PRESENT)
*Mar 21 06:24:16.498: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN)
*Mar 21 06:24:16.498: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
*Mar 21 06:24:16.674: %RF-5-RF_RELOAD: Peer reload. Reason: EHSA standby down
*Mar 21 06:24:16.679: %IOSXE_REDUNDANCY-6-PEER_LOST: Active detected switch 2 is no longer
 standby
*Mar 21 06:24:16.416: %NIF_MGR-6-PORT_LINK_DOWN: Switch 1 R0/0: nif_mgr: Port 1 on front
side stack link 0 is DOWN.
*Mar 21 06:24:16.416: %NIF_MGR-6-PORT_CONN_DISCONNECTED: Switch 1 R0/0: nif_mgr: Port 1 on
 front side stack link 0 connection has DISCONNECTED: CONN_ERR_PORT_LINK_DOWN_EVENT
*Mar 21 06:24:16.416: %NIF_MGR-6-STACK_LINK_DOWN: Switch 1 R0/0: nif_mgr: Front side stack
 link 0 is DOWN.
*Mar 21 06:24:16.416: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack port
1 on Switch 1 is down

<output truncated>

*Mar 21 06:29:36.393: %IOSXE_REDUNDANCY-6-PEER: Active detected switch 2 as standby.
*Mar 21 06:29:36.392: %STACKMGR-6-STANDBY_ELECTED: Switch 1 R0/0: stack_mgr: Switch 2 has
been elected STANDBY.
*Mar 21 06:29:41.397: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_FOUND(4))
*Mar 21 06:29:41.397: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
```

```
 (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
*Mar 21 06:29:42.257: %REDUNDANCY-3-IPC: IOS versions do not match.
*Mar 21 06:30:24.323: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeededFinished
wait for Standby to reach terminal redundancy state


*Mar 21 06:30:25.325: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
STAGE 3: Installing software on Active
==================================================
--- Starting install_active ---
Performing install_active on Chassis 1

<output truncated>

[1] install_active package(s) on switch 1
[1] Finished install_active on switch 1
install_active: Passed on [1]
Finished install_active


STAGE 4: Restarting Active (switchover to standby)
==================================================
--- Starting active reload ---
New software will load after reboot process is completed
SUCCESS: install_add_activate_commit  Thu Mar 21 23:06:45 UTC 2019
Mar 21 23:06:45.731: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot ISSU flash:cat9k_iosxe.16.09.03.SPA.bin
Mar 21 23:06:47.509: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
Mar 21 23:06:48.776: %PM

Initializing Hardware...

System Bootstrap, Version 16.10.1r, RELEASE SOFTWARE (P)
Compiled Fri 08/17/2018 10:48:42.68 by rel

Current ROMMON image : Primary
Last reset cause     : PowerOn
C9500-40X platform with 16777216 Kbytes of main memory

boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf
#
##################################################################################################################


Mar 21 23:08:30.238: %PMAN-5-EXITACTION: C0/0: pvp: Process manager is exiting:

Waiting for 120 seconds for other switches to boot
####################
Switch number is 1
All switches in the stack have been discovered. Accelerating discovery



Switch console is now available


Press RETURN to get started.
```

```
Mar 21 23:14:17.080: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
commit
Mar 21 23:15:48.445: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install commit ISSU
```

Step 10 **show version**

Use this command to verify the version of the new image.

The following sample output of the **show version** command displays the Cisco IOS XE Fuji 16.9.3 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.09.03
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.3, RELEASE
 SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Wed 20-Mar-19 08:02 by mcpre
```

Step 11 **show issu state** [*detail*]

Use this command to verify that no ISSU process is in pending state.

```
Switch# show issu state detail
--- Starting local lock acquisition on chassis 2 ---
Finished local lock acquisition on chassis 2

No ISSU operation is in progress

Switch#
```

Step 12 **exit**

Exits privileged EXEC mode and returns to user EXEC mode.

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	On Cisco Catalyst 9500 Series Switches either **install** commands or **request platform software** commands On Cisco Catalyst 9500 Series Switches - High Performance[5], only **install** commands	

[5] Introduced in Cisco IOS XE Fuji 16.8.1a

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.

```
Switch# request platform software package clean
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.

The following files will be deleted:
[1]:
/flash/cat9k-cc_srdriver.16.06.01..SPA.pkg
/flash/cat9k-espbase.16.06.01.SPA.pkg
/flash/cat9k-guestshell.16.06.01.SPA.pkg
/flash/cat9k-rpbase.16.06.01.SPA.pkg
/flash/cat9k-rpboot.16.06.01.SPA.pkg
/flash/cat9k-sipbase.16.06.01.SPA.pkg
/flash/cat9k-sipspa.16.06.01.SPA.pkg
```

```
/flash/cat9k-srdriver.16.06.01.SPA.pkg
/flash/cat9k-webui.16.06.01.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/cat9k_iosxe.16.06.01.SPA.bin
/flash/packages.conf.00-

Do you want to proceed? [y/n]y
[1]:
Deleting file flash:cat9k-cc_srdriver.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:cat9k_iosxe.16.06.01.SPA.bin ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
Switch#
```

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 2017
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 that the boot variable is set to **flash:packages.conf** and the manual boot variable is set to **no**.

The output should display the following values of these variables:

BOOT variable = **flash:packages.conf**

MANUAL_BOOT variable = no

```
Switch# show boot system
```

Step 4 Software install image to flash

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

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

--- 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
[]: Finished copying to switch
[1]: Expanding file
[1]: Finished expanding all-in-one software package in switch 1
SUCCESS: Finished expanding all-in-one software package.
[1]: 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
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[1]: Finished install successful on switch 1
Checking status of install on [1]
[1]: Finished install in switch 1
SUCCESS: Finished install: Success on [1]
```

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]yBuilding
 configuration...

[OK]Modified configuration has been saved

*Mar 16 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

*Mar 16 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.

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. You should use these commands only if you chose to not reload the system.

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

This step is required only if you install the software image to flash by using the **request platform software package install** command.

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 via “ 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	On Cisco Catalyst 9500 Series Switches, either **install** commands or **request platform software** commands On Cisco Catalyst 9500 Series Switches - High Performance[6], only **install** commands	Cisco IOS XE Fuji 16.9.x or Cisco IOS XE Fuji 16.8.x or Cisco IOS XE Everest 16.x.x release.

[6] Introduced in Cisco IOS XE Fuji 16.8.1a

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.

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.

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

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: Oct 30 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 does not automatically downgrade. It remains 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 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance 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 3: Permitted Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No

Network Advantage	Yes[7]	Yes

[7] 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 9500 Series Switches datasheet at:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/datasheet-c78-738978.html

Limitations and Restrictions

With Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance—If a feature is not supported on a switch model, you do not have to factor in any limitations or restrictions that may be listed here. If limitations or restrictions are listed for a feature that is supported, check if model numbers are specified, to know if they apply. If model numbers are not specified, the limitations or restrictions apply to all models in the series.

- Cisco StackWise Virtual:
  - You cannot configure StackWise Virtual links on the uplink (network) modules (C9500-NM-8X and C9500-NM-2Q).
  - On Cisco Catalyst 9500 Series Switches, you cannot use 4X10G breakout cables or the Cisco QSFP to SFP or SFP+ Adapter (QSA) module when Cisco StackWise Virtual is configured on the switch.
- Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
- Control Plane Policing (CoPP)—The show run command does not display information about classes configured under system-cpp policy, when they are left at default values. Use the show policy-map system-cpp-policy or the show policy-map control-plane commands in privileged EXEC mode instead.
- Flexible NetFlow limitations:
  - You cannot configure NetFlow export using the Ethernet Management port (GigabitEthernet0/0).
  - You can not configure a flow monitor on logical interfaces, such as switched virtual interfaces (SVIs), port-channel, loopback, tunnels.
  - You can not configure multiple flow monitors of same type (ipv4, ipv6 or datalink) on the same interface for same direction.
- Hardware limitations:
  - Use the MODE button to switch-off the beacon LED.
  - All port LED behavior is undefined until interfaces are fully initialized.
  - 1G with Cisco QSA Module (CVR-QSFP-SFP10G) is not supported on the uplink ports of the C9500-24Y4C and C9500-48Y4C models.
  - The following limitations apply to Cisco QSA Module (CVR-QSFP-SFP10G) when Cisco 1000Base-T Copper SFP (GLC-T) or Cisco 1G Fiber SFP Module for Multimode Fiber are plugged into the QSA module:
    - 1G Fiber modules over QSA do not support autonegotiation. Auto-negotiation should be disabled on the far-end devices.

- Although visible in the CLI, the command [**no**] **speed nonegotiate** is not supported with 1G Fiber modules over QSA.
- Only GLC-T over QSA supports auto-negotiation.
- GLC-T supports only port speed of 1000 Mb/s over QSA. Port speeds of 10/100-Mb/s are not supported due to hardware limitation.

- When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, autonegotiation is enabled by default. If the other end of the line does not support autonegotation, the link does not come up.
- Autonegotiation is not supported on HundredGigabitEthernet1/0/49 to HundredGigabitEthernet1/0/52 uplink ports of the C9500-48Y4C models, and HundredGigabitEthernet1/0/25 to HundredGigabitEthernet1/0/28 uplink ports of the C9500-24Y4C models. Disable autonegotiation on the peer device if you are using QSFP-H40G-CUxx and QSFP-H40G-ACUxx cables.
- For QSFP-H100G-CUxx cables, the C9500-48Y4C and C9500-24Y4C models support the cables only if both sides of the connection are either C9500-48Y4C or C9500-24Y4C.

- Interoperability limitations:
  - When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, if one end of the 40G link is a Catalyst 9400 Series Switch and the other end is a Catalyst 9500 Series Switch, the link does not come up, or comes up on one side and stays down on the other. To avoid this interoperability issue between devices, apply the **speed nonegotiate** command on the Catalyst 9500 Series Switch interface. This command disables autonegotiation and brings the link up. To restore autonegotiation, use the **no speed nonegotiation** command.

- In-Service Software Upgrade (ISSU)
  - While performing ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.12.x, if **interface-id snmp-if-index** command is not configured with OSPFv3, packet loss can occur. Configure the **interface-id snmp-if-index** command either during the maintenance window or after isolating the device (by using maintenance mode feature) from the network before doing the ISSU.
  - On Cisco Catalyst 9500 Series Switches (C9500-12Q, C9500-16X, C9500-24Q, C9500-40X), ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.12.x is not supported in the FIPs mode of operation.

- QoS restrictions:
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - For QoS policies, only switched virtual interfaces (SVI) are supported for logical interfaces.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.

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

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

- 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 500 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.
  - Scale—Able to handle up to 5000 bi-directional flows per 24 access ports and 10000 bi-directional flows per 48 access ports.
- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.

Caveats

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

Cisco Bug Search Tool

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

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

Open Caveats in Cisco IOS XE Fuji 16.9.x

Identifier	Applicable Models	Description
CSCvm79234	All Models	Show version cli shows invalid USB-SSD disk size on a CAT9k switch
CSCvq22224	All Models	cat9k // evpn/vxlan // dhcp relay not working over l3vni
CSCve65787	Catalyst 9500 High Performance	Autoneg support for 100G/40G/25G Cu xcvr
CSCvn55969	Catalyst 9500	FED crash when 'show tech nbar' is run
CSCvp31385	Catalyst 9500	Cat9K SVL: Buffer values not changed with qos queue-softmax-multiplier modification
CSCvr90465	All Models	MACSEC link does not recover upon link flap
CSCvs15759	All Models	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

Resolved Caveats in Cisco IOS XE Fuji 16.9.7

Caveat ID Number	Applicable Models	Description
CSCvn22162	All Models	Cat3k crash from corruption in AVL tree
CSCvr77861	All Models	Cat9300/C9500/C9500H switches may reload with last reload reason as LocalSoft or CpuCatastrophicErr
CSCvt30243	Catalyst 9500	Connectivity issue after moving client from dot1x enable port to non dot1x port
CSCvt99266	Catalyst 9500	Memory leak in layer 2 multicast functions
CSCvu35094	All Models	Switch reloads due to fed crash after sending multicast data packets in pvlan
CSCvv48305	Catalyst 9500	Route not fully programmed in the hardware for macsec enabled end-point
CSCvw20578	Catalyst 9500	Switch may reload unexpectedly due to a kernel panic caused by an invalid skb
CSCvw33156	Catalyst 9500	PTP does not work on Twogig interface for 9500-40X-A due to large neighbor propagation delay
CSCvw74061	Catalyst 9500	Cat9300 & Cat9500 series switches may see unexpected reloads due to Localsoft or CpuCatastrophicErr

Resolved Caveats in Cisco IOS XE Fuji 16.9.6

Caveat ID Number	Applicable Models	Description
CSCvk13860	Catalyst 9500	C9K switch does not boot with IOS above 16.8.1a
CSCvm93748	Catalyst 9500	Extra white space for interface in configuration after stackwise interfaces configured
CSCvn98703	All Models	FED_QOS_ERRMSG-3-POLICER_HW_ERROR on Catalyst switches running 16.6 releases
CSCvq23523	All Models	Remove "request platform software trace rotate all" from show tech
CSCvr37805	All Models	Cat3k/9k: Device might reboot after applying "mac address-static xxxx.xxxx.xxxx vlan x drop" command
CSCvr45088	All Models	SVL is not programmed during TCN flood scenario
CSCvr68056	Catalyst 9500 High Performance	Link flap causes negotiation fail of flowcontrol

Caveat ID Number	Applicable Models	Description
CSCvs14641	Catalyst 9500 High Performance	SFPs no longer recognized after OIR
CSCvs14673	Catalyst 9500	SVL node may get removed if one of the SVL links goes bad.
CSCvs50391	All Models	FED crash when premature free of SG element
CSCvs71519	All Models	Switch reloads due to dhcp snooping
CSCvs75010	All Models	Traffic forwarding stops when Session Idle time out is configured 10 sec with active traffic running
CSCvt02962	All Models	Uplink Port-channel Trunk member link Port LED truns to amber blinking after link down/up
CSCvt13518	All Models	QoS ACL matching incorrectly when udp range is used
CSCvt31437	Catalyst 9500	DAD links go into err-disable due to portfast bpduguard global config when both members reload
CSCvt39133	Catalyst 9500	OID cswDistrStackPhyPortInfo triggers memory leak
CSCvt46115	Catalyst 9500 High Performance	C9500H disable stackwise-virtual and related config CLI and show CLI on 16.9.x throttle
CSCvt58704	Catalyst 9500 High Performance	Crash may be seen configuring ptp on Cat9500 series switches
CSCvu15007	All Models	Crash when invalid input interrupts a role-based access-list policy installation
CSCvu37176	All Models	SPAN filter cannot work well when configure FSPAN after 5th session.
CSCvu77091	Catalyst 9500 High Performance	C9500-48Y4C does not resolve ARP with Ethernet SNAP encapsulation

Resolved Caveats in Cisco IOS XE Fuji 16.9.5

Identifier	Applicable Models	Description
CSCvm72574	All models	16.6.4 CPP Police rate wrong in "class system-cpp-police-control-low-priority"
CSCvo81311	All models	FMAN-RP crash observed on Guest Anchor
CSCvp84502	All models	ERSPAN destination does not work or forward traffic

Identifier	Applicable Models	Description
CSCvq05337	All models	Cat3k/9k EGR_INVALID_REWRITE counter increasing in mVPN setup
CSCvq13053	All models	NAT translation entry not cleared after fin-rst time-out
CSCvq22011	All models	IOS-XE drops ARP reply when IPDT gleans from ARP
CSCvq38901	All models	Enable CDP - removed on shut/ no shut dot1Q-tunnel interface
CSCvq50846	All models	ip verify source mac-check prevents device tracking from getting arp probe reply
CSCvq55940	All models	%BIT-4-OUTOFRANGE: bit 4095 is not in the expected range of 1 to 4093
CSCvq66802	All models	igmp query with src ip 0.0.0.0 is not ignored
CSCvq68337	All models	Cat3k/9k does not forward packet when active route down
CSCvq72472	All models	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvq72713	All models	Cat3k/Cat9k can't forwarding traffic follow the rule of EIGRP unequal cost load-balancing
CSCvq75887	All models	intermediate hop with SVI in PIM domain is not forwarding multicast traffic
CSCvq92567	All models	SVL Switchover: standby reloads during bootup
CSCvq94738	All models	The COPP configuration back to the default After rebooting the device
CSCvr03905	All models	Memory Leak on FED due to IPv6 Source Guard
CSCvr04551	All models	Multicast stream flickers on igmp join/leave
CSCvr20522	All models	Cat3k/9k BOOTREPLY dropped when DHCP snooping is enabled
CSCvr23358	All models	Switches are adding Device SGT to proxy generated IGMP leave messages while keeping End host src IP
CSCvr46622	All models	Cat9k || scaled mVPN || tracebacks and errors seen in FED trace
CSCvr46931	All models	ports remain down/down object-manager (fed-ots-mo thread is stuck)
CSCvr48249	All models	High memory utilization under fman_fp_image
CSCvr59959	All models	Cat3k/9k Flow-based SPAN(FSPAN) can only work in one direction when mutilple session configured
CSCvr88090	All models	Cat3k/9k crash on running show platform software fed switch 1 fss abstraction

Identifier	Applicable Models	Description
CSCvr98281	All models	After valid ip conflict, SVI admin down responds to GARP
CSCvr98368	All models	CAT9K intermittently not responding to SNMP
CSCvs14374	All models	16.9.2 ES standby crashed
CSCvs50868	All models	Fed memory leak in 16.9.X related to netflow
CSCvk47894	Catalyst 9500	Cat3k/9k SPAN monitor session works in stack only on adding 2 dest ports in stack
CSCvn78069	Catalyst 9500 High Performance	memory leak @ ngmodslot_get_chassis_id(linux_iosd-imag process).
CSCvs32426	Catalyst 9500 High Performance	Chassis Manager crash occurs when connected to device via RJ-45 console.

Resolved Caveats in Cisco IOS XE Fuji 16.9.4

Caveat ID Number	Applicable Models	Description
CSCvj15473	All models	Linux IOSD crash with sh vtp counters cmd
CSCvj84601	All models	Called-Station-Id attribute not included in Radius Access-Request
CSCvk60809	All models	Wrong Time-Stamp is saved in pcap.
CSCvm80443	All models	IOSd memory leak within DSMIB Server within xqos_malloc_wrapper
CSCvm89543	Catalyst 9500	StackWise-Virtual Ping fails momentarily due to GLC-T optics Link goes up during reboots
CSCvm91107	All models	standby reloads and crashed @fnf_ios_config_dist_validate_sel_process_add
CSCvm91642	All models	MACsec SAP 128 Bits doesn't work with network-essentials license
CSCvn30230	All models	Catalyst 3k/9k: Slow memory leak in linux_iosd-imag
CSCvn57892	All models	High Memory utilization due to Wireless Manager IOSD process
CSCvn69629	All models	ND packets received in remote vtep SISF table - EVPN part
CSCvn99482	All models	IPv6 traffic is stopped on interface when more than 3 invalid ARPs are detected
CSCvo05751	All models	Changes for sending vlan attrs in access request

Caveat ID Number	Applicable Models	Description
CSCvo21122	All models	Memory leak at hman process
CSCvo42353	All models	SDA-External border creating incorrect CEF/map-cache entry due to multicast
CSCvo49876	All models	SISF not honoring 1 IPv4-to-MAC rule when DHCP ACK comes from a different VLAN (via Relay)
CSCvo56629	Catalyst 9500	Interface in Admin shutdown showing incoming traffic and interface Status led in green.
CSCvo57768	All models	NetFlow issue - switch not sending TCP flags
CSCvo60400	All models	errdisable detect cause bpduguard shutdown vlan continues to forward BPDUs
CSCvo61570	All models	spanning-tree uplinkfast max-update-rate's value is abnormal
CSCvo65974	All models	QinQ tunnels causing L2 loop in specific topology of Cat3850
CSCvo66246	All models	Enabling SPAN source of VLAN 1 affects LACP operations
CSCvo71264	All models	Cat3k / Cat9k Gateway routes DHCP offer incorrectly after DHCP snooping
CSCvo73205	All models	Identity policy won't update after config changes.
CSCvo73897	All models	[SDA] [PI changes] No audio during first few seconds of voice call between 2 Fabric Edge
CSCvo75559	All models	First packet not forwarded when (S,G) needs to be built
CSCvo78538	All models	Counters in the "show interface" command are not increasing
CSCvo85422	All models	Directly connected IPv4/IPv6 hosts not programmed in HW - %FMFP-3-OBJ_DWNLD_TO_DP_FAILED
CSCvp00026	All models	[SDA] [PD changes] No audio during first few seconds of voice call between 2 Fabric Edge
CSCvp03816	Catalyst 9500	ENH Hex dump constantly logging when registering access point using DNAC
CSCvp09091	All models	When sourcing Radius from loopback in VRF, auth right out of boot up might fail
CSCvp12187	All models	Standby switch crash due to memory leak due to Switch Integrated Security feature
CSCvp13114	All models	Incoming packet from PVLAN access port is not forwarded out on etherchannel interface

Caveat ID Number	Applicable Models	Description
CSCvp26792	All models	Cat9k control plane impacted when > 1Gbps multicast passes through and no entry in IGMP snooping
CSCvp30629	All models	Cat9300: Lisp site entry count mismatch in external dual border on reload
CSCvp33294	Catalyst 9500	Cat9k || Asic 0 Core 0 buffer stuck, rwePbcStall seen
CSCvp37170	Catalyst 9500	9500-40X Stackwise virtual split after many days
CSCvp49518	All models	DHCP SNOOPING DATABASE IS NOT REFRESHED AFTER RELOAD
CSCvp54779	All models	[SDA] 1st ARP Reply is dropped at remote Fabric Edge
CSCvp65173	All models	SDA: DHCP offer being dropped on BN with L2 and L3 Handoff configured
CSCvp71508	Catalyst 9500 High Performance	Cat9500HP has same mac-address on mgmt port and first asic port after reload
CSCvp72220	All models	crash at sisf_show_counters after entering show device-tracking counters command
CSCvp75221	All models	Modules shows faulty status when specific MAC ACL is applied on interfaces
CSCvp81190	All models	%FED_QOS_ERRMSG-3-TABLEMAP_INGRESS_HW_ERROR was generated after setting policy-map with table-map
CSCvp85601	All models	STP TCN is generated on etherchannel port during a switchover in a switch stack
CSCvp86983	Catalyst 9500	Connectivity over AC tunnel broken due to tunnel deletion from FMAN FP but remains FMAN FP
CSCvp89755	All models	VPN label is wrongly derived as explicit-null in Cat9k for L3 VPN traffic
CSCvp90279	All models	Catalyst switches is sending ADV and REP DHCPv6 packets to SISF when source udp port is not 547
CSCvq29115	Catalyst 9500	Failed to get Board ID shown if stack member boots up
CSCvq30316	All models	[SDA] 1st ARP fix for CSCvp00026 is eventually failing after longevity
CSCvq30460	All models	SYS-2-BADSHARE: Bad refcount in datagram_done - messages seen during system churn

Caveat ID Number	Applicable Models	Description
CSCvq32597	Catalyst 9500 High Performance	C9500 High Performance - Port LED status not displayed correctly
CSCvq40137	All models	Mac address not being learnt when "auth port-control auto" command is present

Resolved Caveats in Cisco IOS XE Fuji 16.9.3

Identifier	Applicable Models	Description
CSCuw36080	All models	SNMP with Extended ACL
CSCvh77984	All models	Router shows "Flash disk quota exceeded" during the reload, but it still has 60% of free memory left
CSCvj79694	All models	sgt-map gets cleared for some of the end points for unknown reason
CSCvk45142	All models	Crash with smd fault on rp_0_0
CSCvm07353	All models	Router may crash when a SSH session is closed after configure TACACS
CSCvm47335	All models	IOSd: large amount of bursty IPC traffic sometime can cause high CPU utilization in fastpath
CSCvm87134	All models	Cat9K stackwise-virtual- Smart license registration status is lost after 2 to 3 multiple reloads/SSO
CSCvm94788	All models	Device reloads when applying #client <IP> vrf Mgmt-vrf server-key 062B0C09586D590B5656390E15
CSCvn02171	All models	HOLE is not created when 'acl default passthrough' configured
CSCvn36494	All models	WCCP redirection to proxy server breaks in certain scenarios.
CSCvn38590	All models	CTS policies download fails with Missing/Incomplete ACEs error
CSCvn58515	All models	Ac Tunnel in "pending-issue-update" state in FMAN FP
CSCvn71041	All models	TACACS group server is not seen, when "transport-map type console test" is configured.
CSCvn72973	All models	Device is getting crashed on the "cts role-based enforcement"
CSCvo00968	All models	Radius attr 32 NAS-IDENTIFIIER not sending the FQDN.
CSCvo17778	All models	Cat9k not updating checksum after DSCP change
CSCvo32446	All models	High CPU Due To Looped Packet and/or Unicast DHCP ACK Dropped

Identifier	Applicable Models	Description
CSCvo33983	All models	Mcast traffic loss seen looks due to missing fed entries during IGMP/MLD snooping.
CSCvi48988	Catalyst 9500	SNMP timeout when querying entSensorValueEntry
CSCvm45417	Catalyst 9500	Cat9K HA/ 16.9.x,16.10.x- Connectivity issue due to wrong dest MAC rewrite for routed packet
CSCvm58577	Catalyst 9500	"%ERROR: Standby doesn't support this command" while configuring standby port
CSCvm77197	Catalyst 9500	C9300 : %IOSXE-2-PLATFORM: Switch 1 R0/0: kernel: EXT2-fs (sda1): error:
CSCvm86478	Catalyst 9500	RMON statistics and RMON MIB absent in cat9K
CSCvn40414	Catalyst 9500	PSU shown as Disabled when there is not input power cables.
CSCvo48808	Catalyst 9500	QSFP-40G-SR4 does not breakout in C9500-16X
CSCvj72988	Catalyst 9500 High Performance	Sometimes FAN removal or insertion is not detected/reported
CSCvn11735	Catalyst 9500 High Performance	"flowcontrol receive off" is not maintained after a reload on interfaces Fuji 16.09.01
CSCvn60882	Catalyst 9500 High Performance	CVR-QSFP-SFP10G V02 May get un-recognised or goes to error disabled state upon installation

Resolved Caveats in Cisco IOS XE Fuji 16.9.2

Identifier	Applicable Models	Description
CSCvg81784	All models	Converting a layer 2 port-channel to L3 causes some Protocols to break
CSCvj16271	All models	Addressing memory leaks in IPC error handling cases in LED, RPS, VMARGIN, USB, THERMAL
CSCvj66609	All models	DHCP offer received from SVI sent back to the same SVI when DHCP Snooping is enabled
CSCvj75719	All models	System returning incorrect portchannel MIB value (IEEE8023-LAG-MIB)
CSCvk53444	All models	Packets with Fragment Offset not forwarded with DHCP Snooping Enabled

Identifier	Applicable Models	Description
CSCvm07921	All models	OOB TX path excessive congestion cause software to force crash a switch
CSCvj74923	Catalyst 9500	Client does not get the reserved IP Address for the interface on Port based DHCP configuration.
CSCvk22204	Catalyst 9500	stackwise virtual will blackhole traffic on standby unit after switchover, NIF is stuck
CSCvk33369	Catalyst 9500	Stack-merge on Stby and CONN_ERR_CONN_TIMEOUT_ERR on Active with multiple SWO
CSCvk33624	Catalyst 9500	SFF8472-3-READ_ERROR message seen for SVL ports
CSCvk59766	Catalyst 9500	QSA adapters using 1 gig SFP stop working
CSCvm36748	Catalyst 9500	FED crash at expired "FED MAC AGING TIMER" or "unknown" timer without a stack trace.
CSCvk35488	Catalyst 9500 High Performance	C9500-24Y4C:"speed 10000" config is rejected on C9500-24Y4C bootup for SFP-10/25GBase-CSR
CSCvk52742	Catalyst 9500 High Performance	1G SFP do not link up when connected to C9500-24Y4C/C9500-48Y4C

Resolved Caveats in Cisco IOS XE Fuji 16.9.1

Identifier	Applicable Models	Description
CSCvh28104	All models	QSFP-H40G-CU5M 40g not showing as up on peer
CSCvh63530	All models	MPLS traffic drops with ECMP loadbalance towards core. All cat9ks
CSCvh96261	All models	EXP based Queuing on cat9k platforms
CSCvj69569	Catalyst 9500	"sh auth sess sw st" broken and session monitoring sessions coming in sh auth sess in legacy mode.
CSCvg53159	Catalyst 9500	%SNMP-3-RESPONSE_DELAYED: processing GetNext of cafSessionEntry.2 seen on catalyst switch
CSCvg58417	Catalyst 9500	Unwanted messages seen during removal of USB 3.0 SSD
CSCvg67012	Catalyst 9500	Deprecate the option of member flash# in upgrade/downgrade CLI for software install
CSCvg95580	Catalyst 9500	interface speed config went lost after same FRU OIR with "write mem"

Identifier	Applicable Models	Description
CSCvh49334	Catalyst 9500	Cat9300 stops forwarding multicast - L3M Failed to allocate REP RI
CSCvh84345	Catalyst 9500	IOS CLI "show platform software fed switch active punt cause summary" may display negative counts
CSCvh87131	Catalyst 9500	TRACEBACK: OID cefcModuleEntry crashes the box
CSCvh92130	Catalyst 9500	downloaded policies hit by traffics were all gone after the second SSO
CSCvi01682	Catalyst 9500	DOM data not available on SFP with QSA adapter when port is shut down
CSCvi08459	Catalyst 9500	set different words for username and password, but username shown the same as password
CSCvi26179	Catalyst 9500	Cat9k crash while accessing OBFL
CSCvi38191	Catalyst 9500	Memory leak in lman process due to "ld_license_ext.dat" build-up.
CSCvi39202	Catalyst 9500	DHCP fails when DHCP snooping trust is enabled on uplink etherchannel
CSCvi71507	Catalyst 9500	C9500: Some SVL can go into P/T state with OIR or HA on some switches
CSCvi75086	Catalyst 9500	Rapid TDL memory leak in SMD process leads to crash of active switch in stack for ipv6 clients
CSCvi75488	Catalyst 9500	Ping from client fails with enforcement enabled on known mappings
CSCvj43609	Catalyst 9500	Incorrect MAC_ADDR gets configured in Rommon
CSCvh77186	Catalyst 9500 High Performance	C9500-32C: Number of PSU fans to be reported correctly in show env status
CSCvh79115	Catalyst 9500 High Performance	C9500-32C: Interfaces takes 5mins to come up after reload
CSCvh09701	Catalyst 9500 High Performance	Power supply state is marked as fail if it is inserted with power cable connected

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 9500 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9500-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.