Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Fuji 16.8.x

First Published: 2018-04-06

Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Fuji 16.8.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 16.8.1a

Hardware Features in Cisco IOS XE Fuji 16.8.1a

- 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 Catalyst 9500 Series Switches—16-port, 10-Gigabit Ethernet switch models	• C9500-16X This model has 16 10-Gigabit Ethernet SFP+ ports and two power supply slots. It supports optional network modules on uplinks ports (An 8-port 10 GigabitEthernet (SFP+) and a 2-port 40 GigabitEthernet (QSFP) network module). • C9500-16X-2Q This model has 16 10-Gigabit Ethernet SFP+ ports and two power supply slots. It supports optional network modules on uplinks ports (A 2-port 40-Gigabit Ethernet (QSFP) network module). See the Cisco Catalyst 9500 Series Switches Hardware Installation Guide.
Cisco 40GBASE-LR4 QSFP module	Supported transceiver module product number: QSFP-40G-LR4-S. 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.

Feature Name	Description
Cisco 4x10GBASE-LR QSFP modules (4x10G breakout mode)	• Supported transceiver module product number—QSFP-4X10G-LR-S • Compatible switch models—C9500-12Q and C9500-24Q (can be installed only on port numbers 1 through 4). • Compatible network modules—C9500-NM-2Q. 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-SR4 QSFP module	Supported transceiver module product number: QSFP-40G-SR4-S 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-SR4 QSFP module (4x10G breakout mode)	• Supported transceiver module product number—QSFP-40G-SR4 • Compatible switch models—C9500-12Q and C9500-24Q (can be installed only on port numbers 1 through 4). • Compatible network modules—C9500-NM-2Q. 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.

Feature Name	Description
Cisco 40-Gigabit Ethernet, QSFP+ Transceiver—QSFP-H40G-AOC	Supported transceiver module product numbers—QSFP-H40G-AOC1M, QSFP-H40G-AOC2M, QSFP-H40G-AOC3M, QSFP-H40G-AOC5M, QSFP-H40G-AOC7M, QSFP-H40G-AOC10M, QSFP-H40G-AOC15M, QSFP-H40G-AOC20M, QSFP-H40G-AOC25M, QSFP-H40G-AOC30M. For information about the module, see the Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Cisco 40-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: C9500-12Q and C9500-24Q 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.

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

Feature Name	Description
Cisco Catalyst 9500 Series Switches - High Performance	High Performance models introduced in the series: • C9500-32C This model has 32 QSFP28 ports that support 40/100 GigabitEthernet connectivity and two power supply slots. • C9500-32QC This model has 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, and two power supply slots. • C9500-48Y4C This model has 48 SFP28 ports that support 1/10/25-GigabitEthernet connectivity, four QSFP uplink ports that support 40/100 -GigabitEthernet connectivity, and two power supply slots. • C9500-24Y4C The model has 24 SFP28 ports that support 1/10/25-GigabitEthernet connectivity, four QSFP uplink ports that support 40/100-GigabitEthernet connectivity, and two power supply slots. See the Cisco Catalyst 9500 Series Switches Hardware Installation Guide.

Feature Name	Description

Power Supply Modules for Cisco Catalyst 9500 Series Switches - High Performance	The following are the supported power supply modules for this series:
	• C9500-32C
	  • C9K-PWR-1600WAC-R — 1600W AC power supply module
	  • C9K-PWR-1600WDC-R— 1600W DC power supply module
	• C9500-32QC
	  • C9K-PWR-650WAC-R — 650W AC power supply module
	  • C9K-PWR-930WDC-R— 930W DC power supply module
	• C9500-48Y4C
	  • C9K-PWR-650WAC-R — 650W AC power supply module
	  • C9K-PWR-930WDC-R— 930W DC power supply module
	• C9500-24Y4C
	  • C9K-PWR-650WAC-R — 650W AC power supply module
	  • C9K-PWR-930WDC-R— 930W DC power supply module
	See the Cisco Catalyst 9500 Series Switches Hardware Installation Guide.

Feature Name	Description
Transceiver Modules and Adapters	The Cisco Catalyst 9500 Series Switches - High Performance support a wide range of optics, some of which are: The Cisco 25-Gigabit Ethernet Transceiver Module (SFP-H25G-CU), the 40-Gigabit Ethernet QSFP+ Transceiver (QSFP-H40G-AOC), the Cisco 40GBASE-LR4 QSFP module (QSFP-40G-LR4-S), the Cisco 40GBASE-SR4 QSFP module (QSFP-40G-SR4-S), QSFP 40G to SFP+ 10G Adapter Module (CVR-QSFP-SFP10G). Consult the tables at this URL for the full list of supported transceivers and compatibility information relating to your device: https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html
M.2 Serial Advanced Technology Attachment (SATA) Solid State Drive (SSD) Module Part numbers: C9K-F1-SSD-240G, C9K-F1-SSD-480G, C9K-F1-SSD-960G	This module is a hot-pluggable drive that can be used for container-based application hosting or as a general mass storage device. Note that it is not meant to be used to store or boot software images. See the Cisco Catalyst 9500 Series Switches Hardware Installation Guide.

Software Features in Cisco IOS XE Fuji 16.8.1a

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

Software Features Introduced on All Models

Feature Name	Description, License Level Information, Documentation Link
DHCPv6: Client Link-Layer Address Option (RFC 6939)	Defines an optional mechanism and the related DHCPv6 option to allow first-hop DHCPv6 relay agents (relay agents that are connected to the same link as the client) to provide the client's link-layer address in the DHCPv6 messages being sent towards the server. (Network Essentials and Network Advantage)
DHCPv6: Support for Option 52 and DNS Search List (DNSSL) Option	Wireless access points use the The Dynamic Host Configuration Protocol version 6 (DHCPv6) option 52 (RFC 5417) to supply the IPv6 management interface addresses of the primary, secondary, and tertiary wireless controllers. The DNSSL option is a list of DNS suffix domain names used by IPv6 hosts when they perform DNS query searches for short, unqualified domain names. The DNSSL option contains one or more domain names. (Network Essentials and Network Advantage)
Support for validation of DHCP Option 125	DHCP option 125 is used by DHCP clients and servers to identify vendor-specific information. Support for validation of DHCP option 125 is enabled if the switch is configured as a DHCP relay agent or if the DHCP snooping feature is turned on. Note that the switch drops those packets that do not conform to the RFC3925 format (HEX format) of option 125.
Hitless ACL Updates (IPv4 and IPv6)	Provides the capability to apply existing features to incoming traffic while updating new features in the TCAM. The feature prevents TCAM reprogramming everytime there is a change in an IPv4 or IPv6 ACL on a given interface. (Network Advantage)

Feature Name	Description, License Level Information, Documentation Link
Media Access Control Security (MACsec): MACsec host link encryption	Support for 128-bit AES MACsec (IEEE 802.1AE) encryption with MACsec Key Agreement (MKA) on downlink ports is enabled. 128-bit—(Network Essentials and Network Advantage)
MACsec: Must-Secure Support for SW-SW MACsec (128-bit and 256-bit encryption)	Support for the must-secure feature is enabled for MKA uplink. With must-secure, all the packets in data traffic are encrypted and unencrypted packets are dropped. • 128-bit—(Network Essentials and Network Advantage) • 256-bit—(Network Advantage)
MACsec enhancements—MACsec Variable length CKN and Optional support for ICV	• MACsec Variable length CKN—Connectivity association key name (CKN) is enhanced to support variable length key-string for 128-bit encryption of MKA-PSK sessions. The range for CKN key-string varies from 1 to 32 hex-digits. • Optional support for ICV—A switch configured with MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the MKA peer. MACsec frames are encrypted and protected with an integrity check value (ICV). Starting with this release, the ICV indicator in the MACsec Key Agreement Protocol Data Unit (MKPDU) is made optional. 128-bit—(Network Essentials and Network Advantage)
Secure Storage of Encryption Keys and Passwords	Secures critical configuration, keys, and passwords by encrypting them. An instance-unique encryption key is stored in the hardware trust anchor to prevent it from being compromised. This feature is enabled on platforms that come with a hardware trust anchor, by default and is not supported on platforms that do not have a hardware trust anchor. (Network Essentials and Network Advantage)

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

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
Audio Video Bridging (AVB): IEEE 802.1BA	Refers to standard IEEE 802.1 BA - AVB. This feature defines a mechanism whereby endpoints and the network function as a whole, to enable high-quality streaming of professional audio and video (AV) over an Ethernet infrastructure. Instead of one-to-one, the network transport enables many-to-many seamless plug-n-play connections for multiple AV endpoints including talkers and listeners. AVB is composed of the following: • Generalized Precision Time Protocol (gPTP)—IEEE 802.1AS. Provides a mechanism to synchronize clocks of the bridges and end point devices in an AVB network. • Quality of Service (QoS)—IEEE 802.1Qav. Guarantees bandwidth and minimum bounded latency for the time-sensitive audio and video streams. • Multiple Stream Reservation Protocol (MSRP)—IEEE 802.1Qat. Provides a mechanism for end stations to reserve network resources that will guarantee the transmission and reception of data streams across a network with the requested bandwidth. • Multiple VLAN Registration Protocol (MVRP)—Provides a mechanism for dynamic maintenance of the contents of Dynamic VLAN Registration Entries for each VLAN ID, and for propagating the information they contain to other Bridges. (Network Advantage)
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. (Network Essentials and Network Advantage)

Feature Name	Description, License Level Information, Documentation Link
Cisco StackWise Virtual	Cisco StackWise Virtual is a network system virtualization technology that pairs two switches into one virtual switch to simplify operational efficiency with a single control and management plane. Starting with this release, the feature is also supported on the following models of the Cisco Catalyst 9500 Series Switches: • C9500-24Q • C9500-12Q • C9500-40X • C9500-16X (Network Advantage)
IGMP packet forwarding in IEEE 802.1Q Tunneling	This enhancement enables Internet Group Management Protocol (IGMP) packet forwarding in IEEE 802.1Q tunnels (Network Essentials and Network Advantage)
IEEE 1588v2, Precision Time Protocol (PTP) support	PTP is defined in IEEE 1588 as Precision Clock Synchronization for Networked Measurements and Control Systems, and was developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability. A PTP profile is the set of allowed PTP features applicable to a device. Only the default profile is available in Cisco IOS XE Fuji 16.8.1. (Network Advantage)
IP-aware Ingress Netflow on VRF Interfaces	IP-aware ingress netflow enables collection of virtual routing and forwarding (VRF) IDs from incoming packets on a device by applying an input flow monitor having a flow record that collects the VRF ID as a key or a non-key field. IP-aware VRF ingress Netflow is supported only on the ingress traffic with IPv4, IPv6 and Multicast Virtual Private Network version 4 (MVPNv4) as Customer Edge Router (CE) facing interface. (Network Advantage)

Feature Name	Description, License Level Information, Documentation Link
IPv6 support for IEEE 802.1Q Tunneling	Enables IPv6 support for the existing 802.1Q tunneling feature. 802.1Q tunneling, also known as Q-in-Q, enables service providers to use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated. A port configured to support 802.1Q tunneling is called a tunnel port. When you configure tunneling, you assign a tunnel port to a VLAN ID that is dedicated to tunneling. (Network Essentials and Network Advantage)
IPv6 support for SGACL Policy Enforcement	Enables IPv6 support for Cisco TrustSec Security Group Access Control List (SGACL) Policy Enforcement. An SGACL associates a Security Group Tag (SGT) with a policy. The policy is enforced upon SGT-tagged traffic egressing the Cisco TrustSec domain. (Network Advantage)
OCSP multiple response handling	Enables support to handle multiple Online Certificate Status Protocol (OCSP) single responses on an OCSP client. (Network Advantage)

Feature Name	Description, License Level Information, Documentation Link
Programmability	

Feature Name	Description, License Level Information, Documentation Link
	• gNMI Operations—Model-driven configuration and retrieval of operational data using the gNMI capabilities, GET and SET RPCs. • Guest Shell Logging and Tracing Support—Provides logging services for guest applications that run separately from the host system, to report tracing data to the host file system. The tracing data is saved in an IOX tracelog and the logging data is saved in the IOS syslog, on the host machine. • IPXE IPv6 support—iPXE IPv6 network boot is supported. • Model Based AAA—Implements the NETCONF Access Control Model (NACM). NACM is a form of role-based access control (RBAC) specified in RFC 6536. • NETCONF Global Session Lock and Kill Session—Provides a global lock and the ability to kill non-responsive sessions in NETCONF. During a session conflict or client misuse of the global lock, NETCONF sessions can be monitored via the **show netconf-yang sessions** command, and non-responsive sessions can be cleared using the clear configuration lock command. • NETCONF and RESTCONF Debug commands—Commands for debugging were added. • NETCONF and RESTCONF IPv6 Support—Data model interfaces (DMIs) support the use of IPv6 protocol. DMI IPv6 support helps client applications to communicate with services that use IPv6 addresses. External facing interfaces will provide dual-stack support; both IPv4 and IPv6. • RESTCONF—Provides an RFC 8040 compliant HTTP-based protocol that provides a programmatic interface for accessing data defined in YANG, using the datastore concepts defined in NETCONF. • YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1681. Revision statements embedded in the YANG files indicate if there has been a model revision. The *README.md* file in the same github location highlights changes that have been made in the release. • Operational Data Parser Polling—Starting with Cisco IOS XE Fuji 16.8.1a, the Operational Data Parser Polling feature is deprecated. All operational data models provide direct operational data model access, hence this feature is no longer required.

Feature Name	Description, License Level Information, Documentation Link
	(Network Essentials and Network Advantage)
Simplified Factory Reset	Removes all customer specific data that has been added to the device since the time of its shipping. Data erased includes configurations, logfiles, bootvariables, corefiles, and credentials. (Network Essentials and Network Advantage)
Transmission Control Protocol (TCP) Maximum Segment Size (MSS) Adjustment	Enables configuration of the maximum segment size for transient packets that traverse the device during a TCP session. (Network Essentials and Network Advantage)
Virtual Ethernet Port Aggregator (VEPA)	Also referred to as reflective relay, the feature moves switching out of the server, back to the physical network, and makes all virtual machine traffic visible to the external network switch. This frees up server resources to support virtual machines. VEPA provides several benefits to Virtual Ethernet Bridge (VEB), which is a physical end station capability that supports local bridging between multiple virtual end stations. (Network Essentials and Network Advantage)
VRF-Aware SGACL Logging	Enables logging of a Virtual Routing and Forwarding (VRF) name in Security Group Access Control List (SGACL) logs, making them VRF aware. (DNA Advantage)

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
Flexible NetFlow: 32 bit AS Number Support	The autonomous system (AS) number space is a 32 bit field with 4,294,967,296 unique values, which are available for use to support the Internet's public inter-domain routing system. The AS number is required to run BGP and peer with your internet service provider, between internet service providers at peering points, and Internet Exchanges (IX). Flexible NetFlow Version 9 and Flexible NetFlow IPFIX export format support the 32 bit AS number. (DNA Essentials)

Feature Name	Description, License Level Information, Documentation Link
Flexible NetFlow: NetFlow v5 Export Protocol	Enables sending of export packets using the Version 5 export protocol. (DNA Essentials)
Lawful Intercept	The process by which law enforcement agencies conduct electronic surveillance as authorized by judicial or administrative order. (Network Advantage)
Protocol Independent Multicast (PIM) Snooping	In networks where a Layer 2 switch interconnects several routers, the switch floods IP multicast packets on all multicast router ports by default, even if there are no multicast receivers downstream. With PIM snooping enabled, the switch restricts multicast packets for each IP multicast group to only those multicast router ports that have downstream receivers joined to that group. (Network Advantage)

Feature Name	Description, License Level Information, Documentation Link
Quality of Service (QoS)	These QoS enhancements were introduced • Sharped Queueing—A queuing mode, which is a combination of shared and shaped queuing modes. The queues share bandwidth according to the configured weights, and are rate-limited to the configured shape-value. • Classification Type: L2-Miss—A classification type that can be set as a criteria to check an incoming packet. L2-Miss can be configured for both source MAC and destination MAC. • L3 Packet Length Classification—Provides the capability to match and classify traffic, based on the Layer 3 packet length in the IP header. The packet length is set as the matching criterion in the class policy-map, to match the value on the incoming packet. • Time-to-Live (TTL)—Also a classification feature. You can set TTL as a criterion in the ACL list, and perform a TTL check on the incoming packet. The access control entry is used to check the IPv4 TTL to match the value on the incoming packet. • Ingress Packet FIFO (IPF)—Parses incoming network traffic to classify frames into different priorities levels. The traffic class is derived from different packet formats. These traffic classes are further mapped to priority levels, which are used to make drop decisions, in case of congestion. • Priority Queue Policer—Supports policing rate on priority queue. Priority queue policer supports only single-rate two-color policing. • Weighted Random Early Detection (WRED) enhancements—Wired ports support a maximum of eight physical queues. You can configure WRED on all the eight physical queues. (Network Essentials and Network Advantage)
Security Group Tag (SGT) Caching	When the switch receives new IP packets with a valid SGT, the switch can now create a cache containing the source IPv4 address, VRF, and SGT bindings. These IP SGT bindings are used to add the Cisco metadata header back to the outgoing packet after deep packet inspection processing. (DNA Advantage)

Feature Name	Description, License Level Information, Documentation Link
Unicast over Point-to-Multipoint GRE and Multicast over Point-to-Multipoint GRE	In a hub-and-spoke topology, multipoint Generic Routing Encapsulation (mGRE) allows multiple destinations to be grouped into a single multipoint interface. It is configured over an IPv4 core or underlying network. (Network Essentials and Network Advantage)
VLAN Translation: One-to-One Mapping	VLAN translation, also known as VLAN mapping, enables service providers to merge two Layer two domains without actually changing their VLAN numbers. (Network Advantage)
Bridge Assurance	Bridge Assurance helps to protect against certain problems that can cause bridging loops in the network. With Bridge Assurance enabled, BPDUs are sent out on all operational network ports for each hello time period. If the port does not receive a BPDU for a specified period, the port is put into a blocked state and is not used in the root port calculation. Once that port receives a BPDU, it resumes the normal spanning tree transitions. Only Rapid PVST+ and MST spanning tree protocols support Bridge Assurance. (Network Essentials)

Important Notes

- Unsupported Features—All Models
- Unsupported Features—Cisco Catalyst 9500 Series Switches
- Unsupported Features—Cisco Catalyst 9500 Series Switches-High Performance

Unsupported Features—All Models

- Bluetooth
- Bidirectional Protocol Independent Multicast (Bidir-PIM)
- Cisco Plug-in for OpenFlow 1.3
- IPsec VPN
- IPsec with FIPS
- 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, 32-bit AS Number Support, TrustSec NetFlow IPv4 Security Group Access Control List (SGACL) Deny and Drop Export
- Gateway Load Balancing Protocol (GLBP)
- In Service Software Upgrade (ISSU)
- 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)
- Ethernet-over-MPLS (EoMPLS) and Pseudowire Redundancy (PWR)
- Virtual Private LAN Service (VPLS) and VPLS BGP-Based Autodiscovery
- External and Internal Border Gateway Protocol (eiBGP) Multipath
- High Availability—Cisco Stackwise Virtual, Graceful Insertion and Removal (GIR), Stateful Switchover (SSO), In Service Software Upgrade (ISSU), 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))
- IPv6 support for Security Group Tag (SGT) and Security Group Access Control Lists (SGACL)
- MPLS Label Distribution Protocol (MPLS LDP) VRF-Aware Static Labels
- Next Generation Network-Based Application Recognition (NBAR) and Next Generation NBAR (NBAR2)
- QoS Options on GRE Tunnel Interfaces
- Software Maintenance Upgrade (SMU)
- Virtual Private LAN Service (VPLS)—VPLS infrastructure, Border Gateway Protocol (BGP) auto discovery for VPLS, L2VPN pseudowire redundancy,

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	
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	
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 16.9.3	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.2	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.1	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.8.1a	2.3 Patch 1 2.4	5.4 5.5	PI 3.3 + PI 3.3 latest maintenance release + PI 3.3 latest device pack See Cisco Prime Infrastructure 3.3→ **Downloads**.
Everest 16.6.4a	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.4	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.3	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**

Catalyst 9500 and 9500-High Performance	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
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	1024 x 768	Small

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

Software Requirements

Operating Systems

- Windows 10 or later
- Mac OS X 10.11 or later

Browsers

- Google Chrome—Version 38 or later (On Windows and Mac)
- Microsoft Edge
- Mozilla Firefox—Version 42 or later (On Windows and Mac)
- Safari—Version 9 or later (On Mac)

Upgrading the Switch Software

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

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

Finding the Software Version

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

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

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

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

Software Images

Release	Image Type	File Name
Cisco IOS XE Fuji 16.8.1a	CAT9K_IOSXE	cat9k_iosxe.16.08.01a.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.08.01a.SPA.bin

Automatic Boot Loader Upgrade

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 16.8.1a first time	The boot loader may be upgraded to version 16.8.1r. For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 16.8.1r [FC4], RELEASE SOFTWARE (P)`
	
	If the automatic boot loader upgrade occurs, while booting Cisco IOS XE Fuji 16.8.1a, you will see the following on the console:
	`%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Tue Mar 13 17:58:44 Universal 2018 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): boot loader upgrade successful`

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 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 16.8.1a
Cisco IOS XE Everest 16.6.2 or Cisco IOS XE Everest 16.6.3	Either **install** commands or **request platform software** commands	

The sample output in this section displays upgrade from

- Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Fuji 16.8.1a using **request platform software** commands.
- Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Fuji 16.8.1a 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 16.8.1a.

```
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 16.8.1a:

```
Switch# install remove inactive

install_remove: START Mon Oct 30 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 Fri Mar 16 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.16.08.01a.SPA.bin flash:

Destination filename [cat9k_iosxe.16.08.01a.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.08.01a.SPA.bin...
```

```
Loading /cat9k_iosxe.16.08.01a.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]

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

b) **dir flash**

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

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

Directory of flash:/

434184 -rw- 601216545 Jul 26 2017 10:18:11 -07:00 cat9k_iosxe.16.08.01a.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

Step 3 Set boot variable

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

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

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

b) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

c) **show boot system**

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

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

```
Switch# show boot system
```

Step 4 Software install image to flash

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

```
Switch# request platform software package install switch all file
flash:cat9k_iosxe.16.08.01a.SPA.bin

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

Expanding image file: flash:cat9k_iosxe.16.08.01a.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.16.08.01a.SPA.pkg
Added cat9k-espbase.16.08.01a.SPA.pkg
Added cat9k-guestshell.16.08.01a.SPA.pkg
Added cat9k-rpbase.16.08.01a.SPA.pkg
Added cat9k-rpboot.16.08.01a.SPA.pkg
Added cat9k-sipbase.16.08.01a.SPA.pkg
Added cat9k-sipspa.16.08.01a.SPA.pkg
Added cat9k-srdriver.16.08.01a.SPA.pkg
Added cat9k-webui.16.08.01a.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]
```

The following sample output displays installation of the Cisco IOS XE Fuji 16.8.1a 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 16.8.1a.

```
Switch# request platform software package install switch all file
flash:cat9k_iosxe.16.08.01a.SPA.bin

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

Expanding image file: flash:cat9k_iosxe.16.08.01a.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.16.08.01a.SPA.pkg
Added cat9k-espbase.16.08.01a.SPA.pkg
Added cat9k-guestshell.16.08.01a.SPA.pkg
Added cat9k-rpbase.16.08.01a.SPA.pkg
Added cat9k-rpboot.16.08.01a.SPA.pkg
Added cat9k-sipbase.16.08.01a.SPA.pkg
Added cat9k-sipspa.16.08.01a.SPA.pkg
```

```
Added cat9k-srdriver.16.08.01a.SPA.pkg
Added cat9k-webui.16.08.01a.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 16.8.1a 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 16.8.1a:

```
Switch# install add file flash:cat9k_iosxe.16.08.01a.SPA.bin activate commit

install_add_activate_commit: START Fri Mar 16 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: Mar 16 19:54:55 install_engine.sh:

%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.08.01a.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.16.08.01a.SPA.bin to the selected switch(es)
Finished initial file syncing

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

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.16.08.01a.SPA.pkg
/flash/cat9k-webui.16.08.01a.SPA.pkg
/flash/cat9k-srdriver.16.08.01a.SPA.pkg
/flash/cat9k-sipspa.16.08.01a.SPA.pkg
/flash/cat9k-sipbase.16.08.01a.SPA.pkg
/flash/cat9k-rpboot.16.08.01a.SPA.pkg
/flash/cat9k-rpbase.16.08.01a.SPA.pkg
/flash/cat9k-guestshell.16.08.01a.SPA.pkg
/flash/cat9k-espbase.16.08.01a.SPA.pkg
/flash/cat9k-cc_srdriver.16.08.01a.SPA.pkg

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

```
[1] Activate package(s) on switch 1
[1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

--- Starting Commit ---
Performing Commit on all members

*Mar 16 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 16 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 Fri Mar 16 19:57:48 UTC 2017
Switch#
```

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

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 16.8.1a:

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

11353194496 bytes total (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 16.8.1a 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  Mar 16 2018 11:49:33 -07:00  cat9k-cc_srdriver.16.08.01a.SPA.pkg
491525 -rw- 78484428  Mar 16 2018 11:49:35 -07:00  cat9k-espbase.16.08.01a.SPA.pkg
491526 -rw- 1598412   Mar 16 2018 11:49:35 -07:00  cat9k-guestshell.16.08.01a.SPA.pkg
491527 -rw- 404153288 Mar 16 2018 11:49:47 -07:00  cat9k-rpbase.16.08.01a.SPA.pkg
491533 -rw- 31657374  Mar 16 2018 11:50:09 -07:00  cat9k-rpboot.16.08.01a.SPA.pkg
491528 -rw- 27681740  Mar 16 2018 11:49:48 -07:00  cat9k-sipbase.16.08.01a.SPA.pkg
491529 -rw- 52224968  Mar 16 2018 11:49:49 -07:00  cat9k-sipspa.16.08.01a.SPA.pkg
491530 -rw- 31130572  Mar 16 2018 11:49:50 -07:00  cat9k-srdriver.16.08.01a.SPA.pkg
491531 -rw- 14783432  Mar 16 2018 11:49:51 -07:00  cat9k-webui.16.08.01a.SPA.pkg
491532 -rw- 9160      Mar 16 2018 11:49:51 -07:00  cat9k-wlc.16.08.01a.SPA.pkg

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

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

- packages.conf—the file that has been re-written with the newly installed .pkg files
- packages.conf.00—backup file of the previously installed image
- cat9k_iosxe.16.08.01a.SPA.conf— a copy of packages.conf and not used by the system.

```
Switch# dir flash:*.conf

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

434197 -rw- 7406 Mar 16 2018 10:59:16 -07:00 packages.conf
434196 -rw- 7504 Mar 16 2018 10:59:16 -07:00 packages.conf.00-
516098 -rw- 7406 Mar 16 2018 10:58:08 -07:00 cat9k_iosxe.16.08.01a.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

Step 6 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

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

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

c) **show version**

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

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

The following sample output of the **show version** command displays the Cisco IOS XE Fuji 16.8.1a image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.08.01a
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.8.1a,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 03-Apr-18 18:49 by mcpre
<output truncated>
```

Downgrading in Install Mode

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

Before you begin

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

When downgrading from ...	Use these commands...	To downgrade to...
Cisco IOS XE Fuji 16.8.1a	Either **install** commands or **request platform software** commands	Cisco IOS XE Everest 16.5.1a or any Cisco IOS XE Everest 16.x.x release.

The sample output in this section shows downgrade from Cisco IOS XE Fuji 16.8.1a to Cisco IOS XE Everest 16.6.1, by using the **install** commands.

Important New switch models that are introduced in this release cannot be downgraded. For the list of models introduced in this release, see Hardware Features in Cisco IOS XE Fuji 16.8.1a, on page 2.

Procedure

Step 1 Clean Up

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 16.8.1a files using the **install remove inactive** command:

```
Switch# install remove inactive

install_remove: START Fri Mar 16 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.16.08.01a.SPA.pkg
/flash/cat9k-espbase.16.08.01a.SPA.pkg
/flash/cat9k-guestshell.16.08.01a.SPA.pkg
/flash/cat9k-rpbase.16.08.01a.SPA.pkg
/flash/cat9k-rpboot.16.08.01a.SPA.pkg
/flash/cat9k-sipbase.16.08.01a.SPA.pkg
/flash/cat9k-sipspa.16.08.01a.SPA.pkg
/flash/cat9k-srdriver.16.08.01a.SPA.pkg
/flash/cat9k-webui.16.08.01a.SPA.pkg
/flash/cat9k-wlc.16.08.01a.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.08.01a.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 Mon Mar 16 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 Mar 16 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 Mon Oct 30 19:54:51 UTC 2017

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

*Oct 30 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

*Mar 16 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 16 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 Fri Mar 16 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.

Using Smart Accounts

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

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

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

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

The possible deployment modes are:

- The right-to-use (RTU) licensing mode—Supported on Cisco Catalyst 9000 Series Switches. See The RTU Licensing Mode.
- The Smart Licensing mode—Currently not supported on Cisco Catalyst 9000 Series Switches. It is on the roadmap for future releases.

The RTU Licensing Mode

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

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

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

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

Options for Base Licenses

```
license right-to-use[{activate|deactivate}][{network-essentials|
network-advantage}][{all|evaluation|subscription{all|slot
<1-8>}}][{acceptEULA}]
```

Options for Add-On Licenses

```
license right-to-use[{activate|deactivate}]addon[{dna-essentials|
dna-advantage}][{all|evaluation|subscription{all|slot <1-8>}}][{acceptEULA}]
```

Usage Guidelines for the RTU Licensing Mode

- Base licenses (Network Essentials and Network-Advantage) may be ordered only with a permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) may be ordered only with a term license type.
- You can set up Cisco SSM to receive daily e-mail alerts, to be notified of expiring add-on licenses that you want to renew.
- You must order an add-on license in order to purchase a switch. On term expiry, you can either renew the add-on license to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- When ordering an add-on license with a base license, note the combinations that are permitted and those that are not permitted:

Table 3: Permitted Combinations

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

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

- The following features are currently available only at the Network Advantage license level. However, the correct minimum license level for these features is Network Essentials and the CFN reflects this correct license level. You will be able to configure these features with a Network Essentials license level after the correction is made in an upcoming release:
  - IPv6 Multicast
  - IPv6 ACL Support for HTTP Servers
- Evaluation licenses cannot be ordered. They can be activated temporarily, without purchase. Warning system messages about the evaluation license expiry are generated 10 and 5 days before the 90-day window. Warning system messages are generated every day after the 90-day period. An expired evaluation license cannot be reactivated after reload.

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

Scaling Guidelines

For information about feature scaling guidelines, see 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 restrictons 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 restrictons apply to all models in the series.

- Cisco StackWise Virtual—When configuring StackWiseVirtual links (SVLs) on the 9500-40X and C9500-16X models of the Cisco Catalyst 9500 Series Switches, note that you cannot create SVLs on any of the uplink modules.
- 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 40GBASE-CR4 QSFP 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.



Note There is no option to turn autonegotiation off on the ports which connect to Cisco 40GBASE-CR4 QSFP cable.

- 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:
  - If one end of the link has a device running Cisco IOS XE Everest 16.6.1 or Cisco IOS XE Everest 16.6.2 or Cisco IOS XE Everest 16.6.3 and the other end is running Cisco IOS XE Fuji 16.8.1a, the link does not come up. To avoid this interoperability issue between releases, it is recommended to use the same image across all the Catalyst 9000 Series Switches in the network.
  - When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, if one end of the 40G link is a Catalyst 9400 Series Switch and the other end is a Catalyst 9500 Series Switch, the link does not come up, or comes up on one side and stays down on the other. To avoid this interoperability issue between devices, apply the the **speed nonegotiate** command on the Catalyst 9500 Series Switch interface. This command disables autonegotiation and brings the link up. To restore autonegotiation, use the **no speed nonegotiation** command.

- 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 16.8.x

Caveat ID Number	Applicable Models	Description
CSCvh63530	All models	MPLS traffic drops with ECMP loadbalance towards core. All cat9ks

Caveat ID Number	Applicable Models	Description
CSCvh72186	All models	Cat9k ROMMON: HTTP booting does not allow specified port number
CSCvi75488	All models	Ping from client fails with enforcement enabled on known mappings
CSCvg90106	Catalyst 9500	[PTP] moving from one TC mode other mode, PTP packets is not forward by TC
CSCvh52491	Catalyst 9500	AVB : FED_QOS_ERRMSG-3-QUEUE_BUFFER_HW_ERROR on shutting down neigh port connected to msrp listener
CSCvg31906	Catalyst 9500	[L3-PTP] TC mode sync/follow up packets are not forward b/w peers for inter vlan communication
CSCvh30574	Catalyst 9500	[SCALE] AVB QoS Crash "Packet Buffer Complex Stalled" with avb/no avb and overnight traffic
CSCvh49334	Catalyst 9500	Cat9300 stops forwarding multicast - L3M Failed to allocate REP RI
CSCvh72645	Catalyst 9500	Policies were failed to be downlaoded from ISE
CSCvh80093	Catalyst 9500	RSTP convergence is taking longer time in certain scenario
CSCvh80485	Catalyst 9500	cts pacs and cts credentials are lost after SSO
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
CSCvh89690	Catalyst 9500	2k dot1x clients authen and classification failedafter SSO on c9400
CSCvg95580	Catalyst 9500	interface speed config went lost after same FRU OIR with "write mem"
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 Cazadero adapter when port is shut down
CSCvi21517	Catalyst 9500	Username is not applying as configured in CAT 9K
CSCvi26179	Catalyst 9500	Cat9k crash while accessing OBFL
CSCvi56916	Catalyst 9500	Cat9500: Will not auto populate MAC_ADDR after unset MAC_ADDR and reset or power cycle.
CSCvi71507	Catalyst 9500	C9500: Some SVL can go into P/T state with OIR or HA on some switches
CSCve65787	Catalyst 9500 High Performance	Autoneg support for 100G/40G/25G Cu xcvr

Caveat ID Number	Applicable Models	Description
CSCvf87541	Catalyst 9500 High Performance	9500: IPv6 multicast traffic does not flow over MGRE tunnel
CSCvg00543	Catalyst 9500 High Performance	Pakcet drop connter at HQoS parent policy or prioritry queue non-HQoS policy
CSCvg23853	Catalyst 9500 High Performance	Hitless update:: seeing packet drop, while modifing ACL by adding VCU ace
CSCvg79227	Catalyst 9500 High Performance	9500H: MGRE Fix TCAM issues for mroutes at scale.
CSCvg79663	Catalyst 9500 High Performance	Unable to scale IPV6 multicast over vrf-lite beyond 25 VRFs
CSCvg84895	Catalyst 9500 High Performance	Seeing little traffic drop even when doing 1 ACE modification in ACL
CSCvh03344	Catalyst 9500 High Performance	Enable OVF memory entry installation for L2
CSCvh09701	Catalyst 9500 High Performance	Power supply state is marked as fail if it is inserted with power cable connected
CSCvh09884	Catalyst 9500 High Performance	Ambiguous cmd when IP option is used for Etherchannel load-balance
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
CSCvh84186	Catalyst 9500 High Performance	Cat9500: SGT caching does not work if egress port is configured as SPAN source port
CSCvh88104	Catalyst 9500 High Performance	IPV6 EC load-balance CLI hashes & reports incorrect Port

Caveat ID Number	Applicable Models	Description
CSCvi06017	Catalyst 9500 High Performance	16.9.1: Asymmetric vlan mapping with MST not working
CSCvi39373	Catalyst 9500 High Performance	BGP neighborship not coming UP with explicit null enabled and traffic punted to CPU

Resolved Caveats in Cisco IOS XE Fuji 16.8.1a

Caveat ID Number	Applicable Models	Description
CSCvh17585	Catalyst 9500	Fed crashes while sending IPv6 traffic with netflow configs
CSCvh31431	Catalyst 9500	Memory leak in linux_iosd-image on 16.6 releases
CSCvh52882	Catalyst 9500	Memory Leak the fed process due nbar config
CSCvh66763	Catalyst 9500	crash is seen at fed_l3_aal_delete_adj
CSCvi19809	Catalyst 9500	Memory leak on C9300 due TMS process
CSCvi69699	Catalyst 9500	9400 - 9300: 40G copper QSFP interoperability broken (link down)
CSCvf77673	Catalyst 9500	Memory leak in OC-Platform

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.

© 2018 Cisco Systems, Inc. All rights reserved.