Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Cupertino 17.7.x

First Published: 2021-12-07

Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Cupertino 17.7.x

Introduction

Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance are leading, fixed, core and aggregation enterprise switching platforms and have been purpose-built to address emerging trends in security, IoT, mobility, and cloud.

These switches 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. This series forms the foundational building block for Software-Defined Access (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 notes document, any such differences are expressly called out. If they are not, the information applies to all the models in the series.

Whats New in Cisco IOS XE Cupertino 17.7.1

Hardware Features in Cisco IOS XE Cupertino 17.7.1

Table 1: Hardware Features Introduced on Cisco Catalyst 9500, 9500X Series and High Performance Switches

Feature Name	Description and Documentation Link
Cisco Catalyst 9500X Series Switches (C9500X-28C8D)	The following new model is introduced in the series: • C9500X-28C8D: 28x100G QSFP28 and 8x400G QSFP-DD ports; 2 power supply slots For information about the hardware including installation and technical specifications, see the Cisco Catalyst 9500X Series Switches Hardware Installation Guide.

Software Features in Cisco IOS XE Cupertino 17.7.1

- Software Features Introduced on All Models, on page 2
- Software Features Introduced on Cisco Catalyst 9500 Series Switches, on page 7
- Software Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance, on page 8

Software Features Introduced on All Models

Feature Name	Description and License Level Information
AAA Authentication Cache for 802.1x	Introduces support for AAA authentication caching for 802.1x.
Cisco TrustSec support with IEEE 802.1X	Introduces support for interoperability of Cisco TrustSec with IEEE 802.1x.
Low priority control packet mapping to Non-Low Latency Queueing (LLQ)	The system generated low-priority CPU traffic is now mapped to threshold 2 of a non-priority queue with highest bandwidth. (Network Essentials)
MACsec Access Control Option	Introduces support for MACsec access control option to allow unencrypted packets to be transmitted or received from the same physical interface.
Mandatory enable secret password in the initial configuration	For a device that loads with no start-up configuration, the enable secret password is now a mandatory configuration in the initial configuration wizard.

Feature Name	Description and License Level Information
MPLS Traffic Engineering • Any Transport over MPLS Tunnel Selection • Forwarding Adjacency • Interarea Tunnels • Inter-AS TE • RSVP Graceful Restart • RSVP Refresh Reduction and Reliable Messaging • Verbatim Path Support	• Any Transport over MPLS Tunnel Selection: Any Transport over MPLS Tunnel Selection feature allows you to specify the path that Any Transport over MPLS (AToM) traffic uses. You can specify either a Multiprotocol Label Switching (MPLS) traffic engineering tunnel or a destination IP address and Domain Name System (DNS) name. • Forwarding Adjacency: Forwarding Adjacency feature allows you to handle a traffic engineering (TE) label switched path (LSP) tunnel as a link in an Interior Gateway Protocol (IGP) network based on the Shortest Path First (SPF) algorithm. • Interarea Tunnels: Interarea Tunnels feature allows you to establish MPLS TE tunnels that span multiple IGP areas and levels, removing the restriction that had required the tunnel headend and tailend devices both to be in the same area. • Inter-AS TE: Autonomous System Boundary Router (ASBR) node protection, loose path reoptimization, stateful switchover (SSO) recovery of label-switched paths (LSPs) that include loose hops. It also provides ASBR forced link flooding, Cisco IOS Resource Reservation Protocol (RSVP) local policy extensions for interautonomous system (Inter-AS), and per-neighbor keys. • RSVP Graceful Restart: RSVP Graceful Restart feature allows a neighboring Route Processor (RP) to recover from disruption in control plane service (specifically, the Label Distribution Protocol (LDP) component) without losing its Multiprotocol Label Switching (MPLS) forwarding state. • RSVP Refresh Reduction and Reliable Messaging: RSVP Graceful Restart feature allows a neighboring Route Processor (RP) to recover from disruption in control plane service (specifically, the Label Distribution Protocol (LDP) component) without losing its Multiprotocol Label Switching (MPLS) forwarding state. • Verbatim Path Support: Verbatim Path Support feature allows network nodes to support Resource Reservation Protocol (RSVP) extensions without supporting Interior Gateway Protocol (IGP) extensions for traffic engineering (TE), thereby bypassing the topology database verification process. (Network Advantage)
PBR support on GRE Tunnel	Allows Policy Based Routing (PBR) to forward traffic on a GRE tunnel. With this, you can configure the next-hop IP address for PBR as a GRE tunnel. (Network Advantage)

Feature Name	Description and License Level Information
Programmability • YANG Model Version 1.1 • Converting IOS Commands to XML • gNOI Factory Reset Services • Leaf-Level Filtering for Telemetry • ZTP Configuration through YANG	The following programmability features are introduced in this release: • YANG Model Version 1.1: Cisco IOS XE Cupertino 17.7.1 uses the YANG version 1.0; however, you can download Cisco IOS XE YANG models in yang-version 1.1 from GitHub at https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1771 folder. For inquiries related to the migrate_yang_version.py script or the Cisco IOS XE YANG version 1.1 migration process, send an email to xe-yang-migration@cisco.com. (Network Advantage) • Converting IOS Commands to XML: This feature helps to automatically translate IOS commands into relevant NETCONF-XML or RESTCONF/JSON request messages. • gNOI Factory Reset Services: The gNOI factory reset service provides an interface that instructs target devices to clean the existing state, and boot the devices in same condition as it was shipped from the factory. (Network Essentials) • Leaf-Level Filtering for Telemetry: Optimised code path is enhanced to support on-change subscriptions via gNMI and gRPC. Both on-change and periodic subscriptions currently receive all the data for the subscribed XPath and all the XPaths under the same gatherpoint. The Leaf-Level Filtering for Telemetry feature allows filtering below the gatherpoint level for the optimized code paths (Network Essentials) • ZTP Configuration through YANG: ZTP is enabled through YANG models when NETCONF is enabled. (Network Essentials)

Feature Name	Description and License Level Information
Smart Licensing Using Policy • Factory-installed trust code • Support for trust code in additional topologies • Ability to save authorization code request and return in a file and simpler upload in the CSSM Web UI • RUM Report optimization and availability of statistics • Support to collect software version in a RUM report • Account information included in the ACK and **show** command outputs • CSLU support for Linux	

Feature Name	Description and License Level Information
	The following Smart Licensing Using Policy enhancements were introduced in this release: • Factory-installed trust code: For new hardware orders, a trust code is now installed at the time of manufacturing. Note: You cannot use a factory-installed trust code to communicate with CSSM. See: Overview and Trust Code. • Support for trust code in additional topologies: A trust code is automatically obtained in topologies where the product instance initiates the sending of data to *CSLU* and in topologies where the product instance is in an air-gapped network. See: • Trust Code • Connected to CSSM Through CSLU and Tasks for Product Instance-Initiated Communication • CSLU Disconnected from CSSM and Tasks for Product Instance-Initiated Communication • No Connectivity to CSSM and No CSLU and Workflow for Topology: No Connectivity to CSSM and No CSLU • Ability to save authorization code request and return in a file and simpler upload in the CSSM Web UI: If your product instance is in an air-gapped network, you can now save a SLAC request in a file on the product instance. The SLAC request file must be uploaded to the CSSM Web UI. You can then download the file containing the SLAC code and install it on the product instance. You can also upload a return request file in a similar manner. With this new method you do not have to gather and enter the required details on the CSSM Web UI to generate a SLAC. You also do not have to locate the product instance in the CSSM Web UI to return an authorization code. In the CSSM Web UI, the request or return file is uploaded in the same location and in the same way as you upload a RUM report. In the required Smart Account, navigate to **Reports** → **Usage Data Files**. See: No Connectivity to CSSM and No CSLU, Workflow for Topology: No Connectivity to CSSM and No CSLU, and license smart (privileged EXEC). • RUM Report optimization and availability of statistics: RUM report generation and related processes have been optimized. This includes a reduction in the time it takes to process RUM reports, better memory and disk space utilization, and visibility into the RUM reports on the product instance (how many there are, the processing state each one is in, if there are errors in any of them, and so on). See: RUM Report and Report Acknowledgement, Upgrades Within the Smart Licensing Using Policy Environment, and Downgrades Within the Smart Licensing Using Policy Environment. Also see: show license rum, show license tech, and show license all. • Support to collect software version in a RUM report: If version privacy is disabled (**no license smart privacy version** global configuration command), the Cisco IOS-XE software version running on the product instance and the Smart Agent version information is *included* in the RUM report.

Feature Name	Description and License Level Information
	See: license smart (global config). • Account information included in the ACK and **show** command outputs: A RUM acknowledgement (ACK) includes the Smart Account and Virtual Account that was reported to, in CSSM. You can then display account information using various **show** commands. The account information that is displayed is always as per the latest available ACK on the product instance. See: show license status, show license summary, show license all, and show license tech. • CSLU support for Linux: CSLU can now be deployed on a machine (laptop or desktop) running Linux. See: CSLU, Workflow for Topology: Connected to CSSM Through CSLU and Workflow for Topology: CSLU Disconnected from CSSM. (Network Advantage)
Switch Integrated Security Features (SISF): ARP Protection	Support for the *prevention* of IPv4 spoofing was introduced (Detection and reporting of IPv4 spoofing is supported since the introductory release of SISF). See: Example: Detecting and Preventing Spoofing.

New on the WebUI
There are no new WebUI features in this release.

Serviceability	
access-session host-mode multi-host peer	The command was modified. **peer** keyword was introduced. Use this command to enable authentication and authorization of a device before any other devices on the fabric edge port. Ensure that the extended node is the peer device that is connected to the fabric edge port.
show ip pim vrf	The command was introduced. It displays Protocol Independent Multicast (PIM) related information for all VRFs.
show ip mroute vrf	The command was introduced. It displays all the multicast VPN routing and forwarding (VRF) instances related to multicast routing tables.
show consistency-checker mcast l3m	The command was modified. **mcast l3m** keyword was introduced. It displays inconsistent states of software entries on the Layer 3 multicast forwarding tables.

Software Features Introduced on Cisco Catalyst 9500 Series Switches

See Software Features Introduced on All Models, on page 2 for features in this release on Cisco Catalyst 9500 Series Switches.

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

Feature Name	Description and License Level Information
AES67 Compliance	Introduces support for AES67 timing profile for high-performance streaming and audio-over-IP interoperability in audio devices. (Network Advantage)

Important Notes

- Unsupported Features: Cisco Catalyst 9500 Series Switches
- Unsupported Features: Cisco Catalyst 9500 Series Switches - High Performance
- Unsupported Features: Cisco Catalyst 9500X Series Switches
- Complete List of Supported Features
- Accessing Hidden Commands
- Default Behaviour—All Models
- Default Interface Behaviour on Cisco Catalyst 9500 Series Switches - High Performance and Cisco Catalyst 9500X Series Switches Only

Unsupported Features: Cisco Catalyst 9500 Series Switches

- **Cisco TrustSec**
  - Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- **Interface and Hardware**
  - Link Debounce Timer
  - M2 SATA Module
  - EnergyWise
- **IP Addressing Services**
  - GRE Redirection
  - VRRPv3: Object Tracking Integration
  - GRE IPv6 Tunnels
  - HSRP and Switch Stack
  - HSRP Groups and Clustering
- **IP Multicast Routing**
  - Unicast over Point-to-Multipoint (P2MP)

- Generic Routing Encapsulation (GRE)
- Multicast over P2MP GRE

- **IP Routing**
  - PIM Bidirectional Forwarding Detection (PIM BFD), PIM Snooping
  - Border Gateway Protocol (BGP) Additional Paths
  - OSPF NSR
  - OSPFv3 NSR
  - OSPFv2 Loop-Free Alternate IP Fast Reroute

- **Layer 2**
  - Audio Engineering Society: AES67 Timing Profile
  - Q-in-Q on a Trunk Port

- **Multiprotocol Label Switching**
  - Hierarchical VPLS with MPLS Access

- **Network Management**
  - 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

- **Quality of Service**
  - Classification (Layer 3 Packet Length, Time-to-Live (TTL))
  - Per queue policer support
  - L2 Miss

- **Security**
  - Lawful Intercept

- **VLAN**
  - QinQ VLAN Mapping

Unsupported Features: Cisco Catalyst 9500 Series Switches - High Performance

- **High Availability**
  - Switch Stacks

- **Interface and Hardware**
  - EnergyWise
- **IP Multicast Routing**
  - IPv6 Multicast and IPv6 Multicast over Point-to-Point GRE
- **IP Routing**
  - Unicast and Multicast over Point-to-Multipoint GRE
  - BFD Multihop Support for IPv4 Static Routes
- **Layer 2**
  - Flexlink+
  - VLAN Load Balancing for FlexLink+
  - Preemption for VLAN Load Balancing
  - FlexLink+ Dummy Multicast Packets
  - Resilient Ethernet Protocol (REP)
- **Multiprotocol Label Switching**
  - MPLS Label Distribution Protocol (MPLS LDP) VRF-Aware Static Labels
  - VPLS Routed Pseudowire IRB(v4) Unicast
- **Network Management**
  - Cisco Application Visibility and Control (AVC)
- **Security**
  - Wake-on-LAN (WoL)
- **System Management**
  - Network-Based Application Recognition (NBAR) and Next-Generation NBAR (NBAR2)

Unsupported Features: Cisco Catalyst 9500X Series Switches

- **Cisco TrustSec**
  - Cisco TrustSec SGT Inline Tagging
  - Cisco TrustSec Manual Configuration
  - Cisco TrustSec Security Association Protocol (SAP)
  - Cisco TrustSec Metadata Header Encapsulation
  - Cisco TrustSec VLAN to SGT Mapping

  - Local Device SGT Mapping
  - IPv6 Support for SGT and SGACL
  - Cisco TrustSec SGT Caching
  - TrustSec SGT Handling: L2 SGT Imposition and Forwarding

- **High Availability**
  - Cisco StackWise Virtual
  - Secure StackWise Virtual
  - Cisco Nonstop Forwarding with Stateful Switchover
  - Graceful Insertion and Removal
  - Switch Stacks

- **Interface and Hardware**
  - Per-port MTU
  - Link Debounce Timer
  - EnergyWise

- **IP Addressing Services**
  - Next Hop Resolution Protocol (NHRP)
  - Network Address Translation (NAT)
  - Web Cache Communication Protocol (WCCP)
  - Switchport Block Unknown Unicast and Switchport Block Unknown Multicast
  - Gateway Load Balancing Protocol (GLBP)
  - Message Session Relay Protocol (MSRP)
  - TCP MSS Adjustment
  - GRE IPv6 Tunnels
  - IP Fast Reroute (IP FRR)

- **IP Multicast Routing**
  - Multicast Routing over GRE Tunnel
  - Multicast VLAN Registration (MVR) for IGMP Snooping
  - IPv6 Multicast over Point-to-Point GRE
  - IGMP Proxy
  - Bidirectional PIM
  - MLD Snooping

- Multicast VPN
- MVPNv6
- mVPN Extranet Support
- MLDP-Based VPN
- PIM Snooping
- PIM Dense Mode

- **IP Routing**
  - OSPFv2 Loop-Free Alternate IP Fast Reroute
  - EIGRP Loop-Free Alternate IP Fast Reroute
  - Policy-Based Routing (PBR)
  - PBR for IPv6
  - VRF-Aware PBR
  - Local PBR
  - Multipoint GRE
  - Web Cache Communication Protocol (WCCP)

- **Layer 2**
  - Multi-VLAN Registration Protocol (MVRP)
  - Loop Detection Guard
  - Cross-Stack UplinkFast
  - Optional Spanning Tree Protocol
  - Precision Time Protocol (PTP)
  - Audio Engineering Society: AES67 Timing Profile
  - PTPv2 on Cisco StackWise Virtual
  - Fast UniDirectional Link Detection
  - UniDirectional Link Detection (UDLD)
  - IEEE 802.1Q Tunneling
  - One-to-One VLAN Mapping
  - Selective Q-in-Q
  - Q-in-Q on a Trunk Port
  - Audio Video Bridging (AVB): IEEE 802.1BA
  - Flexlink+

- VLAN Load Balancing for FlexLink+
- Preemption for VLAN Load Balancing
- FlexLink+ Dummy Multicast Packets
- Resilient Ethernet Protocol (REP)
- Resilient Ethernet Protocol

- **Multiprotocol Label Switching**
  - BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN
  - MPLS over GRE
  - MPLS Layer 2 VPN over GRE
  - MPLS Layer 3 VPN over GRE
  - Virtual Private LAN Service (VPLS)
  - VPLS Autodiscovery, BGP-based
  - VPLS Layer 2 Snooping: Internet Group Management Protocol or Multicast Listener Discovery
  - Hierarchical VPLS with Multiprotocol Label Switching Access
  - VPLS Routed Pseudowire IRB(v4) Unicast
  - MPLS VPN Inter-AS Options (options A, B, and AB)
  - MPLS VPN Inter-AS IPv4 BGP Label Distribution
  - Seamless Multiprotocol Label Switching

- **Network Management**
  - ERSPAN and RSPAN
  - Flow-Based Switch Port Analyser
  - FRSPAN
  - Egress Netflow
  - IP Aware MPLS Netflow
  - NetFlow Version 5

- **Quality of Service**
  - QoS Ingress Shaping
  - VPLS QoS
  - Microflow Policers
  - Per VLAN Policy and Per Port Policer
  - Mixed COS/DSCP Threshold in a QoS LAN-queueing Policy

- Easy QoS: match-all Attributes
- Classify: Packet Length
- Class-Based Shaping for DSCP/Prec/COS/MPLS Labels
- CoPP Microflow Policing
- Egress Policing
- Egress Microflow Destination-Only Policing
- Ethertype Classification
- Packet Classification Based on Layer3 Packet-Length
- PACLs
- Per IP Session QoS
- Per Queue Policer
- QoS Data Export
- QoS L2 Missed Packets Policing

- **Security**
  - Lawful Intercept
  - MACsec:
    - Switch-to-host MACsec
    - Cisco TrustSec Security Association Protocol
    - Fallback Key
    - MACsec EAP-TLS
  - MAC ACLs
  - Port ACLs
  - VLAN ACLs
  - IP Source Guard
  - IPv6 Source Guard
  - Web-based Authentication
  - Port Security
  - Weighted Random Early Detection mechanism (WRED) Based on DSCP, PREC, or COS
  - IEEE 802.1x Port-Based Authentication

- **System Management**
  - Unicast MAC Address Filtering

- **VLAN**
  - Wired Dynamic PVLAN
  - Private VLANs

Complete List of Supported Features

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

Choose the following in the context of the Cisco Catalyst 9500 Series Switches:

- 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
- CAT9500X: to see all the features supported on the C9500X-28C8D model

Accessing Hidden Commands

From 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. That is, entering a question mark (?) at the system prompt did not display the list of available commands. Hidden commands are only meant to assist Cisco TAC in advanced troubleshooting, and are not documented either.

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

- Category 1: Hidden commands in Privileged or User EXEC mode. Enter the **service internal** command to access these commands.
- Category 2: Hidden commands in one of the configuration modes (global, interface, and so on).

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

- The commands have CLI help. Enter a question mark (?) at the system prompt to display 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 a hidden command is used. The following is an 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 categories 1 and 2, there are other internal commands displayed on the CLI, for which the system does *not* generate the `%PARSER-5-HIDDEN` syslog message.

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

If you find that you need to use 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 nonhidden commands.

Default Behaviour—All Models

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

Default Interface Behaviour on Cisco Catalyst 9500 Series Switches - High Performance and Cisco Catalyst 9500X Series Switches Only

From Cisco IOS XE Gibraltar 16.11.1, the default interface for all High Performance and 9500X models in the series changes from Layer 3 to Layer 2. Use the **no switchport** command to change the Layer 2 interface into Layer 3 mode.

The startup configuration has explicit configuration of the **switchport** command for Layer 2 interfaces and the **no switchport** command for Layer 3 interfaces to address this change in behaviour and to support seamless migration.

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 2: 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 3: 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.

Table 4: Cisco Catalyst 9500X Series Switches

Switch Model	Default License Level[3]	Description
C9500X-28C8D-E	Network Essentials	28x100G QSFP28 and 8x400G QSFP-DD ports; two power supply slots
C9500X-28C8D-A	Network Advantage	
C9500X-60L4D-A	Network Advantage	60x50G SFP56 and 4x400G QSFP-DD ports; two power supply slots

[3] 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 between Cisco Catalyst 9500 Series Switches, Cisco Identity Services Engine, Cisco Access Control Server, and Cisco Prime Infrastructure.

Catalyst 9500, 9500-High Performance and 9500X	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Cupertino 17.7.1	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.8	3.2 Patch 4	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.7	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.6a	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.6	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.

Catalyst 9500, 9500-High Performance and 9500X	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Bengaluru 17.6.5	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.4	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.3	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.2	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.1	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Bengaluru 17.5.1	3.0 Patch 1 2.7 Patch 2 2.6 Patch 7 2.4 Patch 13	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.

Catalyst 9500, 9500-High Performance and 9500X	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Bengaluru 17.4.1	3.0 2.7 Patch 2	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Amsterdam 17.3.8a	2.7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Amsterdam 17.3.8	2.7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Amsterdam 17.3.7	2.7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Amsterdam 17.3.6	2.7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Amsterdam 17.3.5	2.7	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Amsterdam 17.3.4	2.7	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Amsterdam 17.3.3	2.7	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.

Catalyst 9500, 9500-High Performance and 9500X	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Amsterdam 17.3.2a	2.7	-	PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See Cisco Prime Infrastructure 3.8 → **Downloads**.
Amsterdam 17.3.1	2.7	-	PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See Cisco Prime Infrastructure 3.8 → **Downloads**.
Amsterdam 17.2.1	2.7	-	PI 3.7 + PI 3.7 latest maintenance release + PI 3.7 latest device pack See Cisco Prime Infrastructure 3.7 → **Downloads**.
Amsterdam 17.1.1	2.7	-	PI 3.6 + PI 3.6 latest maintenance release + PI 3.6 latest device pack See Cisco Prime Infrastructure 3.6 → **Downloads**.
Gibraltar 16.12.8	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.7	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.6	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.5b	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.

Catalyst 9500, 9500-High Performance and 9500X	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.12.5	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.4	2.6	-	PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See Cisco Prime Infrastructure 3.8 → Downloads.
Gibraltar 16.12.3a	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.3	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.2	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.1	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.11.1	2.6 2.4 Patch 5	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**.
Gibraltar 16.10.1	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.

Catalyst 9500, 9500-High Performance and 9500X	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**.

Catalyst 9500, 9500-High Performance and 9500X	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Fuji 16.8.1a	2.3 Patch 1 2.4	5.4 5.5	PI 3.3 + PI 3.3 latest maintenance release + PI 3.3 latest device pack See Cisco Prime Infrastructure 3.3→ **Downloads**.
Everest 16.6.4a	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.4	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.3	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
Everest 16.6.2	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
Everest 16.6.1	2.2	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
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[4]	512 MB[5]	256	1280 x 800 or higher	Small

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

Software Requirements

Operating Systems

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

Browsers

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

ROMMON Versions

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

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

ROMMON upgrades may be required to resolve firmware defects, or to support new features, but there may not be new versions with every release.

The following table provides ROMMON version information for the Cisco Catalyst 9500 Series Switches. For ROMMON version information of Cisco IOS XE 16.x.x releases, refer to the corresponding Cisco IOS XE 16.x.x release notes of the respective platform.

Release	ROMMON Version (C9500-12Q, C9500-24Q, C9500-16X, C9500-40X)	ROMMON Version (C9500-32C, C9500-32QC, C9500-24Y4C, C9500-48Y4C)	ROMMON Version (C9500X)
Cupertino 17.7.1	17.6.1r[FC1]	17.6.1r	-
Bengaluru 17.6.8	17.6.1r[FC1]	17.6.1r	-
Bengaluru 17.6.7	17.6.1r[FC1]	17.6.1r	-
Bengaluru 17.6.6a	17.6.1r[FC1]	17.6.1r	-
Bengaluru 17.6.6	17.6.1r[FC1]	17.6.1r	-
Bengaluru 17.6.5	17.6.1r[FC1]	17.6.1r	-
Bengaluru 17.6.4	17.6.1r[FC1]	17.6.1r	-

Release	ROMMON Version (C9500-12Q, C9500-24Q, C9500-16X, C9500-40X)	ROMMON Version (C9500-32C, C9500-32QC, C9500-24Y4C, C9500-48Y4C)	ROMMON Version (C9500X)
Bengaluru 17.6.3	17.6.1r[FC1]	17.6.1r	-
Bengaluru 17.6.2	17.6.1r[FC1]	17.6.1r	-
Bengaluru 17.6.1	17.6.1r[FC1]	17.6.1r	-
Bengaluru 17.5.1	17.5.1r	17.3.1r[FC2]	-
Bengaluru 17.4.1	17.4.1r	17.3.1r[FC2]	-
Amsterdam 17.3.8a	17.3.1r[FC2]	17.3.1r[FC2]	-
Amsterdam 17.3.8	17.3.1r[FC2]	17.3.1r[FC2]	-
Amsterdam 17.3.7	17.3.1r[FC2]	17.3.1r[FC2]	-
Amsterdam 17.3.6	17.3.1r[FC2]	17.3.1r[FC2]	-
Amsterdam 17.3.5	17.3.1r[FC2]	17.3.1r[FC2]	-
Amsterdam 17.3.4	17.3.1r[FC2]	17.3.1r[FC2]	-
Amsterdam 17.3.3	17.3.1r[FC2]	17.3.1r[FC2]	-
Amsterdam 17.3.2a	17.3.1r[FC2]	17.3.1r[FC2]	-
Amsterdam 17.3.1	17.3.1r[FC2]	17.3.1r[FC2]	-
Amsterdam 17.2.1	17.2.1r[FC1]	17.1.1[FC2]	-
Amsterdam 17.1.1	17.1.1r [FC1]	17.1.1[FC1]	-

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 Cupertino 17.7.1	CAT9K_IOSXE	cat9k_iosxe.17.07.01.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.07.01.SPA

Upgrading the ROMMON

To know the ROMMON or bootloader version that applies to every major and maintenance release, see ROMMON Versions, on page 26.

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

- Upgrading the ROMMON in the primary SPI flash device

  On the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the series, *you must manually upgrade* the ROMMON in the primary SPI flash device, if a new version is applicable, and the release you are upgrading *from* is Cisco IOS XE Gibraltar 16.12.1 or a later release. (So if you upgrade from Cisco IOS XE Gibraltar 16.11.1 for example, a manual upgrade does not apply; the ROMMON is automatically updated, if applicable). Enter the **upgrade rom-monitor capsule primary switch** command in privileged EXEC mode.

  On the C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C models of the series, this ROMMON is upgraded automatically. When you upgrade from an existing release on your switch to a later or newer release for the first time, and there is a new ROMMON version in the new release, the system automatically upgrades the ROMMON in the primary SPI flash device, based on the hardware version of the switch.

- Upgrading the ROMMON in the golden SPI flash device

  You must manually upgrade this ROMMON. The manual upgrade applies to all models in the series. Enter the **upgrade rom-monitor capsule golden switch** command in privileged EXEC mode.

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

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

Software Installation Commands

Summary of Software Installation Commands **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, using **install** commands, in install mode. To perform a software image upgrade, you must be booted into IOS through **boot flash:packages.conf**.

Before you begin

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 Cupertino 17.7.x
Cisco IOS XE Everest 16.6.2 and all later releases	On Cisco Catalyst 9500 Series Switches, either **install** commands or **request platform software** commands[6]. On Cisco Catalyst 9500 Series Switches - High Performance, only install commands[7].	

[6] The **request platform software** commands are deprecated. So although they are still visible on the CLI, we recommend that you use **install** commands.
[7] Introduced in Cisco IOS XE Fuji 16.8.1a.

The sample output in this section displays upgrade from Cisco IOS XE Bengaluru 17.6.1 to Cisco IOS XE Cupertino 17.7.1 using **install** commands only.

Procedure

Step 1 Clean-up

install remove inactive

Use this command to clean-up old installation files in case of insufficient space and to ensure that you have at least 1GB of space in flash, to expand a new image.

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command:

```
Switch# install remove inactive
install_remove: START Wed Jul 21 19:51:48 UTC 2021
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
    cat9k-cc_srdriver.17.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-espbase.17.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-guestshell.17.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpbase.17.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpboot.17.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipbase.17.06.01.SPA.pkg
      File is in use, will not delete.
```

```
    cat9k-sipspa.17.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-srdriver.17.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-webui.17.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-wlc.17.06.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.
The following files will be deleted:
[R0]:
/flash/cat9k-cc_srdriver.17.06.01.SPA.pkg
/flash/cat9k-espbase.17.06.01.SPA.pkg
/flash/cat9k-guestshell.17.06.01.SPA.pkg
/flash/cat9k-rpbase.17.06.01.SPA.pkg
/flash/cat9k-rpboot.17.06.01.SPA.pkg
/flash/cat9k-sipbase.17.06.01.SPA.pkg
/flash/cat9k-sipspa.17.06.01.SPA.pkg
/flash/cat9k-srdriver.17.06.01.SPA.pkg
/flash/cat9k-webui.17.06.01.SPA.pkg
/flash/cat9k-wlc.17.06.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[R0]:
Deleting file flash:cat9k-cc_srdriver.17.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.17.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.17.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.17.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.17.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.17.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.17.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.17.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.17.06.01.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 Wed Jul 21 19:52:25 UTC 2021
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp:***[[//location]/directory]/filename***flash:**

Use this command to copy the new image from a TFTP server to flash memory. The location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers. Skip this step if you want to use the new image from a TFTP server.

```
Switch# copy tftp://10.8.0.6/image/cat9k_iosxe.17.07.01.SPA.bin flash:
destination filename [cat9k_iosxe.17.07.01.SPA.bin]?
Accessing tftp://10.8.0.6/image/cat9k_iosxe.17.07.01.SPA.bin...
Loading /cat9k_iosxe.17.07.01.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 23 2021 10:18:11 -07:00 cat9k_iosxe.17.07.01.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
```

b) **no boot manual**

Use this command to configure the switch to auto-boot. Settings are synchronized with the standby switch, if applicable.

```
Switch(config)# no boot manual
Switch(config)# exit
```

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show bootvar** or **show boot**

Use this command to verify the boot variable (packages.conf) and manual boot setting (no):

```
Switch# show bootvar               <<on the C9500-24Y4C,C9500-32C, C9500-32QC, and
C9500-48Y4C models
BOOT variable = bootflash:packages.conf
MANUAL_BOOT variable = no
BAUD variable = 9600
ENABLE_BREAK variable = yes
BOOTMODE variable does not exist
IPXE_TIMEOUT variable does not exist
CONFIG_FILE variable =

Standby BOOT variable = bootflash:packages.conf
Standby MANUAL_BOOT variable = no
Standby BAUD variable = 9600
Standby ENABLE_BREAK variable = yes
Standby BOOTMODE variable does not exist
Standby IPXE_TIMEOUT variable does not exist
Standby CONFIG_FILE variable =

Switch# show boot                        <<on the C9500-12Q,C9500-16X C9500-24Q, and
C9500-40X models
Current Boot Variables:
BOOT variable = flash:packages.conf;
```

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

Step 4 Install image to flash

install add file activate commit

Use this command to install the image.

We recommend that you point to the source image on your TFTP server or the flash drive of the *active* switch, if you have copied the image to flash memory. If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For example, if the image is on the flash drive of member switch 3 (flash-3): `Switch# install add file flash-3:cat9k_iosxe.17.07.01.SPA.bin activate commit`.

The following sample output displays installation of the Cisco IOS XE Cupertino 17.7.1 software image in the flash memory:

```
Switch# install add file flash:cat9k_iosxe.17.07.01.SPA.bin activate commit
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....
--- Starting Add ---
Performing Add on Active/Standby
 [1] Add package(s) on R0
 [1] Finished Add on R0

Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.7.01

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.07.01.SPA.pkg
/flash/cat9k-webui.17.07.01.SPA.pkg
/flash/cat9k-srdriver.17.07.01.SPA.pkg
/flash/cat9k-sipspa.17.07.01.SPA.pkg
/flash/cat9k-sipbase.17.07.01.SPA.pkg
/flash/cat9k-rpboot.17.07.01.SPA.pkg
/flash/cat9k-rpbase.17.07.01.SPA.pkg
/flash/cat9k-guestshell.17.07.01.SPA.pkg
/flash/cat9k-espbase.17.07.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.07.01.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n] y

--- Starting Activate ---

Performing Activate on Active/Standby
[1] Activate package(s) on R0
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k-cc_srdriver.17.06.01.SPA.pkg
      Removed cat9k-espbase.17.06.01.SPA.pkg
      Removed cat9k-guestshell.17.06.01.SPA.pkg
      Removed cat9k-rpbase.17.06.01.SPA.pkg
      Removed cat9k-rpboot.17.06.01.SPA.pkg
      Removed cat9k-sipbase.17.06.01.SPA.pkg
```

```
      Removed cat9k-sipspa.17.06.01.SPA.pkg
      Removed cat9k-srdriver.17.06.01.SPA.pkg
      Removed cat9k-webui.17.06.01.SPA.pkg
      Removed cat9k-wlc.17.06.01.SPA.pkg
    New files list:
      Added cat9k-cc_srdriver.17.07.01.SSA.pkg
      Added cat9k-espbase.17.07.01.SSA.pkg
      Added cat9k-guestshell.17.07.01.SSA.pkg
      Added cat9k-lni.17.07.01.SSA.pkg
      Added cat9k-rpbase.17.07.01.SSA.pkg
      Added cat9k-rpboot.17.07.01.SSA.pkg
      Added cat9k-sipbase.17.07.01.SSA.pkg
      Added cat9k-sipspa.17.07.01.SSA.pkg
      Added cat9k-srdriver.17.07.01.SSA.pkg
      Added cat9k-webui.17.07.01.SSA.pkg
      Added cat9k-wlc.17.07.01.SSA.pkg
    Finished list of software package changes
  [1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on Active/Standby
  [1] Commit package(s) on R0
  [1] Finished Commit on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit
Send model notification for install_add_activate_commit before reload
Install will reload the system now!
SUCCESS: install_add_activate_commit  Wed Jul 21 12:13:05 IST 2021

Switch#Jul 21 12:13:11.023: %PMANTACTION: F0/0vp: Process manager is exiting: n requested
Jul 21 12:13:11.028: %PMAN-5-EXITACTION: C1/0: pvp: Process manager is exiting: reload fru
 action requested
Jul 21 12:13:11.825: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload
action requested

Initializing Hardware...
System Bootstrap, Version 17.4.1r[FC2], RELEASE SOFTWARE (P)

Compiled 30-04-2021 12:00:00.00 by rel
Current ROMMON image : Primary Rommon Image
Last reset cause:LocalSoft
C9500-32QC platform with 16777216 Kbytes of main memory
Preparing to autoboot. [Press Ctrl-C to interrupt]  5     5     /-\|/-\|/-4     \|/-\|/-\|3
     /-\|/-\|/-2     \|/-\|/-\|1     /-\|/-\|/-0

boot: attempting to boot from [bootflash:packages.conf]

boot: reading file packages.conf
<output truncated>
```

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 Verify installation

After the software has been successfully installed, use the **dir flash:** command to verify that the flash partition has ten new `.pkg` files and two `.conf` files.

a) **dir flash:*.pkg**

The following is sample output of the **dir flash:*.pkg** command:

```
Switch# dir flash:*.pkg

Directory of flash:/
475140 -rw- 2012104   Mar 18 2021 09:52:41 -07:00 cat9k-cc_srdriver.17.06.01.SPA.pkg
475141 -rw- 70333380  Mar 18 2021 09:52:44 -07:00 cat9k-espbase.17.06.01.SPA.pkg
475142 -rw- 13256     Mar 18 2021 09:52:44 -07:00 cat9k-guestshell.17.06.01.SPA.pkg
475143 -rw- 349635524 Mar 18 2021 09:52:54 -07:00 cat9k-rpbase.17.06.01.SPA.pkg
475149 -rw- 24248187  Mar 18 2021 09:53:02 -07:00 cat9k-rpboot.17.06.01.SPA.pkg
475144 -rw- 25285572  Mar 18 2021 09:52:55 -07:00 cat9k-sipbase.17.06.01.SPA.pkg
475145 -rw- 20947908  Mar 18 2021 09:52:55 -07:00 cat9k-sipspa.17.06.01.SPA.pkg
475146 -rw- 2962372   Mar 18 2021 09:52:56 -07:00 cat9k-srdriver.17.06.01.SPA.pkg
475147 -rw- 13284288  Mar 18 2021 09:52:56 -07:00 cat9k-webui.17.06.01.SPA.pkg
475148 -rw- 13248     Mar 18 2021 09:52:56 -07:00 cat9k-wlc.17.06.01.SPA.pkg

491524 -rw- 25711568  Jul 23 2021 11:49:33 -07:00 cat9k-cc_srdriver.17.07.01.SPA.pkg
491525 -rw- 78484428  Jul 23 2021 11:49:35 -07:00 cat9k-espbase.17.07.01.SPA.pkg
491526 -rw- 1598412   Jul 23 2021 11:49:35 -07:00 cat9k-guestshell.17.07.01.SPA.pkg
491527 -rw- 404153288 Jul 23 2021 11:49:47 -07:00 cat9k-rpbase.17.07.01.SPA.pkg
491533 -rw- 31657374  Jul 23 2021 11:50:09 -07:00 cat9k-rpboot.17.07.01.SPA.pkg
491528 -rw- 27681740  Jul 23 2021 11:49:48 -07:00 cat9k-sipbase.17.07.01.SPA.pkg
491529 -rw- 52224968  Jul 23 2021 11:49:49 -07:00 cat9k-sipspa.17.07.01.SPA.pkg
491530 -rw- 31130572  Jul 23 2021 11:49:50 -07:00 cat9k-srdriver.17.07.01.SPA.pkg
491531 -rw- 14783432  Jul 23 2021 11:49:51 -07:00 cat9k-webui.17.07.01.SPA.pkg
491532 -rw- 9160      Jul 23 2021 11:49:51 -07:00 cat9k-wlc.17.07.01.SPA.pkg
11353194496 bytes total (9544245248 bytes free)
Switch#
```

b) **dir flash:*.conf**

The following is sample output of the **dir flash:*.conf** command. It displays the .conf files in the flash partition; note the two .conf files:

- `packages.conf`—the file that has been re-written with the newly installed .pkg files
- `cat9k_iosxe.17.07.01.SPA.conf`— a backup copy of the newly installed packages.conf file

```
Switch# dir flash:*.conf

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

434197 -rw- 7406 Jul 23 2021 10:59:16 -07:00 packages.conf
516098 -rw- 7406 Jul 23 2021 10:58:08 -07:00 cat9k_iosxe.17.07.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

Step 6 **show version**

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

The following sample output of the **show version** command displays the Cisco IOS XE Cupertino 17.7.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.07.01
Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.7.1,
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
<output truncated>
```

Downgrading in Install Mode

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

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 Cupertino 17.7.x	• On Cisco Catalyst 9500 Series Switches, either **install** commands or **request platform software** commands[8]. • On Cisco Catalyst 9500 Series Switches - High Performance, only **install** commands	Cisco IOS XE Bengaluru 17.6.x or earlier releases.

[8] The **request platform software** commands are deprecated. So although they are still visible on the CLI, we recommend that you use **install** commands.

Note New switch models that are introduced in a release cannot be downgraded. The release in which a switch model is introduced is the minimum software version for that model.

The sample output in this section shows downgrade from Cisco IOS XE Cupertino 17.7.1 to Cisco IOS XE Bengaluru 17.6.1, using **install** commands.

Procedure

Step 1 Clean-up

install remove inactive

Use this command to clean-up old installation files in case of insufficient space and to ensure that you have at least 1GB of space in flash, to expand a new image.

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command:

```
Switch# install remove inactive
 install_remove: START Wed Jul 21 11:42:27 IST 2021

Cleaning up unnecessary package files

No path specified, will use booted path bootflash:packages.conf

Cleaning bootflash:
  Scanning boot directory for packages ... done.
```

```
  Preparing packages list to delete ...
    cat9k-cc_srdriver.17.07.01.SSA.pkg
      File is in use, will not delete.
    cat9k-espbase.17.07.01.SSA.pkg
      File is in use, will not delete.
    cat9k-guestshell.17.07.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpbase.17.07.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpboot.17.07.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipbase.17.07.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipspa.17.07.01.SSA.pkg
      File is in use, will not delete.
    cat9k-srdriver.17.07.01.SSA.pkg
      File is in use, will not delete.
    cat9k-webui.17.07.01.SSA.pkg
      File is in use, will not delete.
    cat9k-wlc.17.07.01.SSA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.
SUCCESS: No extra package or provisioning files found on media. Nothing to clean.

SUCCESS: install_remove  Wed Jul 21 11:42:39 IST 2021
```

Step 2 Copy new image to flash

a) **copy tftp:***[[//location]/directory]/filename***flash:**

Use this command to copy the new image from a TFTP server to flash memory. The location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers. Skip this step if you want to use the new image from a TFTP server.

```
Switch# copy tftp://10.8.0.6/image/cat9k_iosxe.17.06.01.SPA.bin flash:
Destination filename [cat9k_iosxe.17.06.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.17.06.01.SPA.bin...
Loading /cat9k_iosxe.17.06.01.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 21 2021 13:35:16 -07:00 cat9k_iosxe.17.06.01.SPA.bin
11353194496 bytes total (9055866880 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
```

b) **no boot manual**

Use this command to configure the switch to auto-boot. Settings are synchronized with the standby switch, if applicable.

```
Switch(config)# no boot manual
Switch(config)# exit
```

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show bootvar** or **show boot**

Use this command to verify the boot variable (packages.conf) and manual boot setting (no):

```
Switch# show bootvar                <<on the C9500-24Y4C,C9500-32C, C9500-32QC, and
C9500-48Y4C models
BOOT variable = bootflash:packages.conf
MANUAL_BOOT variable = no
BAUD variable = 9600
ENABLE_BREAK variable = yes
BOOTMODE variable does not exist
IPXE_TIMEOUT variable does not exist
CONFIG_FILE variable =

Standby BOOT variable = bootflash:packages.conf
Standby MANUAL_BOOT variable = no
Standby BAUD variable = 9600
Standby ENABLE_BREAK variable = yes
Standby BOOTMODE variable does not exist
Standby IPXE_TIMEOUT variable does not exist
Standby CONFIG_FILE variable =
```

```
Switch# show boot                          <<on the C9500-12Q,C9500-16X C9500-24Q, and
C9500-40X models
Current Boot Variables:
BOOT variable = flash:packages.conf;

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

Step 4 Downgrade software image

install add file activate commit

Use this command to install the image.

We recommend that you point to the source image on your TFTP server or the flash drive of the *active* switch, if you have copied the image to flash memory. If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For example, if the image is on the flash drive of member switch 3 (flash-3): `Switch# install add file flash-3:cat9k_iosxe.17.06.01.SPA.bin activate commit`.

The following example displays the installation of the Cisco IOS XE Bengaluru 17.6.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.17.06.01.SPA.bin activate commit
install_add_activate_commit: Adding PACKAGE
```

```
install_add_activate_commit: Checking whether new add is allowed ....
--- Starting Add ---
Performing Add on Active/Standby
[1] Add package(s) on R0
[1] Finished Add on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add
Image added. Version: 17.06.01.0.269
install_add_activate_commit: Activating PACKAGE

Following packages shall be activated:
/flash/cat9k-wlc.17.06.01.SPA.pkg
/flash/cat9k-webui.17.06.01.SPA.pkg
/flash/cat9k-srdriver.17.06.01.SPA.pkg
/flash/cat9k-sipspa.17.06.01.SPA.pkg
/flash/cat9k-sipbase.17.06.01.SPA.pkg
/flash/cat9k-rpboot.17.06.01.SPA.pkg
/flash/cat9k-rpbase.17.06.01.SPA.pkg
/flash/cat9k-guestshell.17.06.01.SPA.pkg
/flash/cat9k-espbase.17.06.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.06.01.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n] y


Performing Activate on Active/Standby
1] Activate package(s) on R0
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k-cc_srdriver.17.07.01.SSA.pkg
      Removed cat9k-espbase.17.07.01.SSA.pkg
      Removed cat9k-guestshell.17.07.01.SSA.pkg
      Removed cat9k-lni.17.07.01.SSA.pkg
      Removed cat9k-rpbase.17.07.01.SSA.pkg
      Removed cat9k-rpboot.17.07.01.SSA.pkg
      Removed cat9k-sipbase.17.07.01.SSA.pkg
      Removed cat9k-sipspa.17.07.01.SSA.pkg
      Removed cat9k-srdriver.17.07.01.SSA.pkg
      Removed cat9k-webui.17.07.01.SSA.pkg
      Removed cat9k-wlc.17.07.01.SSA.pkg
    New files list:
      Added cat9k-cc_srdriver.17.06.01.SPA.pkg
      Added cat9k-espbase.17.06.01.SPA.pkg
      Added cat9k-guestshell.17.06.01.SPA.pkg
      Added cat9k-rpbase.17.06.01.SPA.pkg
      Added cat9k-rpboot.17.06.01.SPA.pkg
      Added cat9k-sipbase.17.06.01.SPA.pkg
      Added cat9k-sipspa.17.06.01.SPA.pkg
      Added cat9k-srdriver.17.06.01.SPA.pkg
      Added cat9k-webui.17.06.01.SPA.pkg
      Added cat9k-wlc.17.06.01.SPA.pkg
    Finished list of software package changes
  [1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on Active/Standby
 [1] Commit package(s) on R0
 [1] Finished Commit on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
```

```
Finished Commit

Send model notification for install_add_activate_commit before reload
Install will reload the system now!
SUCCESS: install_add_activate_commit  Wed Jul 21 11:51:01 IST 2021

Jul 21 11:51:07.505: %PMANTvp: Process manager is exiting: ren requested
Jul 21 11:51:07.505: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fru
 action requested
Jul 21 11:51:07.834: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload
action requested

Initializing Hardware...

System Bootstrap, Version 17.3.1r[FC2], RELEASE SOFTWARE (P)
Compiled 30-04-2021 12:00:00.00 by rel
Current ROMMON image : Primary Rommon Image

Last reset cause:LocalSoft
C9500-32QC platform with 16777216 Kbytes of main memory
Preparing to autoboot. [Press Ctrl-C to interrupt]  5     5     /-\|/-\|/-4     \|/-\|/-\|3
     /-\|/-\|/-2     \|/-\|/-\|1     /-\|/-\|/-0
boot: attempting to boot from [bootflash:packages.conf]
boot: reading file packages.conf

<output truncated>
```

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 Verify version

show version

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

Note
When you downgrade the software image, the ROMMON version does not downgrade. It remains updated.

The following sample output of the **show version** command displays the Cisco IOS XE Bengaluru 17.6.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.06.01
Cisco IOS Software [Bengaluru], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.6.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
<output truncated>
```

Field-Programmable Gate Array Version Upgrade

A field-programmable gate array (FPGA) is a type of programmable memory device that exists on Cisco switches. They are re-configurable logic circuits that enable the creation of specific and dedicated functions.

To check the current FPGA version, enter the **version -v** command in ROMMON mode.

Note

- Not every software release has a change in the FPGA version.
- The version change occurs as part of the regular software upgrade and you do not have to perform any other additional steps.

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.

Available Licensing Models and Configuration Information

- Cisco IOS XE Fuji 16.8.x and earlier: RTU Licensing is the default and the only supported method to manage licenses.
- Cisco IOS XE Fuji 16.9.1 to Cisco IOS XE Amsterdam 17.3.1: Smart Licensing is the default and the only supported method to manage licenses.

Note On the Cisco Catalyst 9500 Series Switches-High Performance, it is from Cisco IOS XE Fuji 16.8.1a to Cisco IOS XE Amsterdam 17.3.1.

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

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

  For more information, see Configuring Licenses on Cisco Catalyst 9000 Series Switches.

For a more detailed overview on Cisco Licensing, go to Cisco Software Licensing Guide.

License Levels - Usage Guidelines

- The duration or term for which a purchased license is valid:

Smart Licensing Using Policy	Smart Licensing
• Perpetual: There is no expiration date for such a license. • Subscription: The license is valid only until a certain date (for a three, five, or seven year period).	• 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.

- Base licenses (Network Essentials and Network-Advantage) are ordered and fulfilled only with a perpetual or permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a subscription or 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 5: Permitted Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No
Network Advantage	Yes[9]	Yes

[9] 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*.

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.

- Auto negotiation

  Auto negotiation (the **speed auto** command) and half duplex (the **duplex half** command) are not supported on GLC-T or GLC-TE transceivers for 10 Mbps and 100 Mbps speeds. This applies only to the C9500-48Y4C and C9500-24Y4C models of the series.

  We recommend not changing Forward Error Correction (FEC) when auto negotiation is ON. This is applicable to 100G/40G/25G CU cables on the C9500-32C, C9500-32QC, C9500-24Y4C and C9500-48Y4C models of the series.

- Control Plane Policing (CoPP)—The **show run** command does not display information about classes configured under `system-cpp policy`, when they are left at default values. Use the **show policy-map system-cpp-policy** or the **show policy-map control-plane** commands in privileged EXEC mode instead.

- Cisco StackWise Virtual

  - On Cisco Catalyst 9500 Series Switches, when Cisco StackWise Virtual is configured, breakout ports using 4X10G breakout cables, or the Cisco QSFP to SFP or SFP+ Adapter (QSA) module can only be used as data ports; they cannot be used to configure StackWise Virtual links (SVLs) or dual-active detective (DAD) links.

  - On Cisco Catalyst 9500 Series Switches - High Performance,

    - When Cisco StackWise Virtual is configured, breakout ports using 4X25G or 4X10G breakout cables can only be used as data ports; they cannot be used to configure SVLs or DAD links.

    - When Cisco StackWise Virtual is configured, Cisco QSA module with 10G SFP modules can be used as data ports and to configure SVLs or DAD links.

    - When Cisco StackWise Virtual is configured, Cisco QSA module with 1G SFP modules can be used as data ports and to configure DAD links; they cannot be used to configure SVLs since SVLs are not supported on 1G interfaces.

- Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.

- Flexible NetFlow limitations

  - You cannot configure NetFlow export using the Ethernet Management port (GigabitEthernet0/0).

- You can not configure a flow monitor on logical interfaces, such as layer 2 port-channels, loopback, tunnels.
- You can not configure multiple flow monitors of same type (ipv4, ipv6 or datalink) on the same interface for same direction.

- Hardware Limitations — Optics:
  - 1G with Cisco QSA Module (CVR-QSFP-SFP10G) is not supported on the uplink ports of the C9500-24Y4C and C9500-48Y4C models.
  - Installation restriction for SFP-10G-T-X module on C9500-24Y4C and C9500-48Y4C— Only eight SFP-10G-T-X modules are supported at a time. If you insert a ninth SFP-10G-T-X module in a lower numbered port than the existing active eight SFP-10G-T-X module, a reload will bring up the ninth transceiver and moves the last existing port with SFP-10G-T-X module to error disabled state. This happens due to the order of sequence ports link bring up where the lower numbered port brings up the link first. This limitation applies in standalone and in Cisco StackWise Virtual setup with two C9500-24Y4C or C9500-48Y4C switches. Each switch can have eight SFP-10G-T-X modules.

    The following error displays on the console if you insert a ninth module with eight active modules:

    ```
    "%IOMD_ETHER_GEIM-4-MAX_LIMIT_XCVR: R0/0: iomd: Number of
    SFP-10G-T-X that can be supported has reached the max limit of 8,
     transceiver is err-disabled. Unplug the transceiver in interface
     TwentyFiveGigE1/0/29
    ```

  - SFP-10G-T-X supports 100Mbps/1G/10G speeds based on auto negotiation with the peer device. You cannot force speed settings from the transceiver.

- Hardware limitations:
  - Use the MODE button to switch-off the beacon LED.
  - All port LED behavior is undefined until interfaces are fully initialized.
  - 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.
- For C9500-32C model, the power supply with serial number starting with POG has two fans and the power supply with serial number starting with QCS has a single fan. When you use **show environment status** command, the fan status of one fan is always displayed as `N/A` when the power supply with single fan is installed into the power supply slot. See Configuring Internal Power Supplies.

- Interoperability limitations—When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, if one end of the 40G link is a Catalyst 9400 Series Switch and the other end is a Catalyst 9500 Series Switch, the link does not come up, or comes up on one side and stays down on the other. To avoid this interoperability issue between devices, apply the the **speed nonegotiate** command on the Catalyst 9500 Series Switch interface. This command disables autonegotiation and brings the link up. To restore autonegotiation, use the **no speed nonegotiation** command.
- In-Service Software Upgrade (ISSU)
  - In-Service Software Upgrade (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 16.10.x or to Cisco IOS XE Gibraltar 16.11.x is not supported.
  - On Cisco Catalyst 9500 Series Switches - High Performance (C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C), ISSU with Cisco StackWise Virtual is supported only starting from Cisco IOS XE Gibraltar 16.12.1. Therefore, ISSU upgrades can be performed only starting from this release to a later release.
  - While ISSU allows you to perform upgrades with zero downtime, we recommend you to do so during a maintenance window only.
  - If a new feature introduced in a software release requires a change in configuration, the feature should not be enabled during ISSU.
  - If a feature is not available in the downgraded version of a software image, the feature should be disabled before initiating ISSU.
- QoS restrictions
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - Policing and marking policy on sub interfaces is supported.
  - Marking policy on switched virtual interfaces (SVI) is supported.
  - 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.

- Smart Licensing Using Policy: Starting with Cisco IOS XE Amsterdam 17.3.2a, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

  The licensing utilities and user interfaces that are affected by this limitation include only the following: Cisco Smart Software Manager (CSSM), Cisco Smart License Utility (CSLU), and Smart Software Manager On-Prem (SSM On-Prem).

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

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

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

- MACsec is not supported on Software-Defined Access deployments.

- 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.
- Embedded Event Manager—Identity event detector is not supported on Embedded Event Manager.
- On the C9500X-28C8D model of the Cisco Catalyst 9500 Series Switches, TCAM space will not be reserved for different features. The available TCAM space will be shared across the features.
- The File System Check (fsck) utility is not supported in install mode.
- Switch Web UI allows configuration of data VLANs only and not voice VLANs. If you remove a voice VLAN configured to an interface using the Web UI, then all data VLANs associated with the interface are also removed by default.

Caveats

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

Cisco Bug Search Tool

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

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

Open Caveats in Cisco IOS XE Cupertino 17.7.x

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Cupertino 17.7.1

Identifier	Applicable Models	Description
CSCvs33050	All models	SVL Hung - CPU HOG by Process - "Crimson Flush Transaction"
CSCvx87277	All models	Cat9k may experience an unexpected reboot with Critical process fed fault on fp_0_0
CSCvy16234	All models	IOSd crashes with system buffer pool corruption
CSCvy08148	All models	Multicast packets replicates twice after redundant switch take power off
CSCvy25845	All models	SNMP: ifHCInOctets - snmpwalk on sub-interface octet counter does not increase
CSCvy51582	All models	SNMP: sub-interface octet counter reports wrong value

Identifier	Applicable Models	Description
CSCvy62453	All models	Cat9k Switch may see Multicast traffic loss triggered by IGMP Join received on Mcast source port.
CSCvz54210	All models	C9300 / C9500 / C9500H // Constraining Uncore Frequency on CPU to mitigate Hang/Crash
CSCvy25356	Catalyst 9500	Packet leak from L2 flooding-enabled fabric IP Pools into L2 Border external VLAN
CSCvz18383	Catalyst 9500	SGT Bindings for Fabric Enabled SSIDs are not seen on Fabric Edge Switch
CSCvt16172	Catalyst 9500 High Performance	Wrong values for transceivers (DOM) in Cat9k Core switches
CSCvx94276	Catalyst 9500 High Performance	%CRIMSON-3-DATABASE_MEMLEAK: Database memory leak detected in /tmp/rp/tdldb/0/IOS_PRIV_OPER_DB

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: https://cfnng.cisco.com/mibs

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

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

© 2021 Cisco Systems, Inc. All rights reserved.