Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Cupertino 17.7.x

First Published: 2021-12-07

Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Cupertino 17.7.x

Introduction

Cisco Catalyst 9600 Series Switches are the next generation purpose-built 40 GigabitEthernet, 50 GigabitEthernet, 100 GigabitEthernet, and 400 GigabitEthernet modular core and aggregation platform providing resiliency at scale with the industry's most comprehensive security while allowing your business to grow at the lowest total operational cost. They have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

They deliver hardware and software convergence in terms of ASIC architecture with Unified Access Data Plane (UADP) 3.0 and Cisco Silicon One Q200. The platform runs an Open Cisco IOS XE that supports model driven programmability, Serial Advanced Technology Attachment (SATA) Solid State Drive (SSD) local storage, and a higher memory footprint). The series forms the foundational building block for SD-Access, which is Cisco's lead enterprise architecture.

It also supports features that provide high availability, advanced routing and infrastructure services, security capabilities, and application visibility and control.

Whats New in Cisco IOS XE Cupertino 17.7.1

Hardware Features in Cisco IOS XE Cupertino 17.7.1

Feature Name	Description and Documentation Link
Cisco Catalyst 9600 Series Supervisor Engine 2 (C9600X-SUP-2)	This supervisor engine is supported on Cisco Catalyst 9600 Series 6 Slot Chassis (C9606R). It has two 10G SFP+ management ports. One port is used for management and the other port can be used to connect to any port on the line cards. These two ports only support 10G SFP+ transceivers. Compatible line cards: • C9600-LC-40YL4CD • C9600-LC-24C • C9600-LC-48YL • C9600-LC-48TX For more information about the hardware, see the Cisco Catalyst 9600 Series Supervisor Engine Installation Note and Cisco Catalyst 9600 Series Switches Hardware Installation Guide. For more information about supported software features, see Software Configuration Guide, Cisco IOS XE Cupertino 17.7.x (Catalyst 9600 Switches) and Command Reference, Cisco IOS XE Cupertino 17.7.x (Catalyst 9600 Switches).
C9600-LC-40YL4CD	Cisco Catalyst 9600 Series 40-Port 50G, 2-Port 200G, 2-Port 400G Line Card. It supports: • 40 SFP56 ports, 2 QSFP56 ports and 2 QSFP-DD ports. SFP56 ports support 50G or 25G or 10G, whereas QSFP56 ports support 200G/100G/40G and QSFP-DD ports support 400G/200G/100G/40G speeds. • 40 ports of 50G/25G/10G, 2 ports of 200G/100G/40G and 2 ports of 400G/200G/100G/40G with C9600X-SUP-2 • 40 ports of 25G/10G/1G and 2 ports of 100G/40G with C9600-SUP-1 For more information about the hardware, see Cisco Catalyst 9600 Series Line Card Installation Note.

Software Features in Cisco IOS XE Cupertino 17.7.1

Feature Name	Description and License Level Information
AAA Authentication Cache for 802.1x	Introduces support for AAA authentication caching for 802.1x.
AES67 Compliance	Introduces support for AES67 timing profile for high-performance streaming and audio-over-IP interoperability in audio devices.

Feature Name	Description and License Level Information
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.
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.
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.
PBR support on GRE Tunnel	Allows Policy Based Routing (PBR) to forward traffic on a GRE tunnel. With this, the next-hop IP address for PBR can be a GRE tunnel.

Feature Name	Description and License Level Information
Programmability • YANG Model Version 1.1 • Converting IOS Commands to XML • 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. • Converting IOS Commands to XML: This feature helps to automatically translate IOS commands into relevant NETCONF-XML or RESTCONF/JSON request messages. • 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 • ZTP Configuration through YANG: ZTP is enabled through YANG models when NETCONF is enabled.
PTPv2 and gPTP without Stateful Switchover (SSO)	Introduces support for Precision Time Protocol (PTP) and Generalized PTP (gPTP) without SSO. PTP is defined in IEEE 1588v2 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. gPTP is an IEEE 802.1 AS standard, that provides a mechanism to synchronize the clocks of the bridges and end-point devices in a network. (Network Advantage)

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**. 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.
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 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.

Important Notes

Unsupported Features: Cisco Catalyst 9600 Series Supervisor 2 Module

- **Cisco Trustsec**
  - Cisco TrustSec Manual Configuration
  - Cisco TrustSec Security Association Protocol (SAP)
  - Cisco TrustSec Metadata Header Encapsulation

- IPv6 Support for SGT and SGACL
- Cisco TrustSec SGT Caching
- TrustSec SGT Handling: L2 SGT Imposition and Forwarding
- Cisco TrustSec SGT Inline Tagging

- **High Availability**
  - Quad-Supervisor with Route Processor Redundancy
  - Cisco StackWise Virtual
  - Secure StackWise Virtual

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

- **IP Addressing Services**
  - Next Hop Resolution Protocol (NHRP)
  - Network Address Translation (NAT)
  - Gateway Load Balancing Protocol (GLBP)
  - Web Cache Communication Protocol (WCCP)
  - Switchport Block Unknown Unicast and Switchport Block Unknown Multicast
  - 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
  - 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)
  - VRF-Aware PBR
  - Local PBR
  - PBR for Object-Group Access Control List (OGACL) Based Matching
  - Multipoint GRE
  - Web Cache Communication Protocol (WCCP)
  - Unicast and Multicast over Point-to-Multipoint GRE

- **Layer 2**
  - Multi-VLAN Registration Protocol (MVRP)
  - Loop Detection Guard

- **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 MPLS 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:
    - MACsec EAP-TLS
    - Switch-to-host MACsec
    - Certificate-based MACsec
    - Cisco TrustSec SAP MACsec

    - 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.

Accessing Hidden Commands

This section provides information about hidden commands in Cisco IOS XE and the security measures that are in place, when they are accessed. These commands are only meant to assist Cisco TAC in advanced troubleshooting and are not documented.

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. Enter 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. 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.

Default Behaviour

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).

Supported Hardware

Cisco Catalyst 9600 Series Switches—Model Numbers

The following table lists the supported switch models. For information about the available license levels, see section *License Levels*.

Switch Model (append with "=" for spares)	Description
C9606R	Cisco Catalyst 9606R Switch • Redundant supervisor module capability • Four linecard slots • Hot-swappable fan tray, front and rear serviceable, fan tray assembly with 9 fans. • Four power supply module slots

Supported Hardware on Cisco Catalyst 9600 Series Switches

Product ID (append with "=" for spares)	Description
Supervisor Modules	
C9600-SUP-1	Cisco Catalyst 9600 Series Supervisor 1 Module This supervisor module is supported on the C9606R chassis.

Product ID (append with "=" for spares)	Description
C9600X-SUP-2	Cisco Catalyst 9600 Series Supervisor Engine 2 This supervisor module is supported on the C9606R chassis.
SATA[1] SSD[2] Modules (for the Supervisor)	
C9K-F2-SSD-240GB	Cisco Catalyst 9600 Series 240GB SSD Storage
C9K-F2-SSD-480GB	Cisco Catalyst 9600 Series 480GB SSD Storage
C9K-F2-SSD-960GB	Cisco Catalyst 9600 Series 960GB SSD Storage
Line Cards	
C9600-LC-40YL4CD	Cisco Catalyst 9600 Series 40-Port SFP56, 2-Port QSFP56, 2-Port QSFP-DD line card. • C9600X-SUP-2 • 40 SFP56 ports of 50G/25G/10G • 2 QSFP56 ports of 200G/100G/40G • 2 QSFP-DD ports of 400G/200G/100G/40G • C9600X-SUP-1 • 40 SFP28 ports of 25G/10G/1G • 2 QSFP28 ports of 100G/40G
C9600-LC-48YL	Cisco Catalyst 9600 Series 48-Port SFP56 line card. • C9600X-SUP-2 • 48 SFP56 ports of 50G/25G/10G • C9600X-SUP-1 • 48 SFP28 ports of 25G/10G/1G
C9600-LC-24C	Cisco Catalyst 9600 Series 24-Port 40G/12-Port 100G line card. • C9600X-SUP-2 • 24 QSFP28 ports of 100G/40G • C9600-SUP-1 • 12 ports of 100G or 24 ports of 40G

Product ID (append with "=" for spares)	Description
C9600-LC-48TX	Cisco Catalyst 9600 Series 48-Port MultiGigabit RJ45 line card. • C9600X-SUP-2 • 48 ports of 10G/5G/2.5G • C9600X-SUP-1 • 48 ports of 10G/5G/2.5G/1G and 100M/10M
C9600-LC-48S	Cisco Catalyst 9600 Series 48-Port SFP line card. • C9600X-SUP-2 • Not supported • C9600-SUP-1 • 48 SFP ports of 1G
AC Power Supply Modules	
C9600-PWR-2KWAC	Cisco Catalyst 9600 Series 2000W AC Power Supply Module[3]
DC Power Supply Modules	
C9600-PWR-2KWDC	Cisco Catalyst 9600 Series 2000W DC Power Supply Module

1 Serial Advanced Technology Attachment (SATA)
2 Solid State Drive (SSD) Module
3 Power supply output capacity is 1050W at 110 VAC.

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 9600 Series Switches, Cisco Identity Services Engine, Cisco Access Control Server, and Cisco Prime Infrastructure.

Catalyst 9600	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 17.6.7	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**.
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**.

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
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**.
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**.

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
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**.
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	-	-
Gibraltar 16.12.8	2.6	-	-
Gibraltar 16.12.7	2.6	-	-

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.12.6	2.6	-	-
Gibraltar 16.12.5b	2.6	-	-
Gibraltar 16.12.5	2.6	-	-
Gibraltar 16.12.4	2.6	-	-
Gibraltar 16.12.3a	2.6	-	-
Gibraltar 16.12.3	2.6	-	-
Gibraltar 16.12.2	2.6	-	-
Gibraltar 16.12.1	2.6	-	-
Gibraltar 16.11.1	2.6 2.4 Patch 5	5.4 5.5	-
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**.
Fuji 16.9.8	2.5 2.1	5.4 5.5	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.7	2.5 2.1	5.4 5.5	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.6	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.5	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Fuji 16.9.4	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.8.1a	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 9600 Series Supervisor Modules. 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 (C9600-SUP-1)	ROMMON Version (C9600X-SUP-2)
Cupertino 17.7.1	17.6.1r	17.7.1r[FC3]
Bengaluru 17.6.7	17.6.1r	-
Bengaluru 17.6.6a	17.6.1r	-
Bengaluru 17.6.6	17.6.1r	-
Bengaluru 17.6.5	17.6.1r	-
Bengaluru 17.6.4	17.6.1r	-
Bengaluru 17.6.3	17.6.1r	-

Release	ROMMON Version (C9600-SUP-1)	ROMMON Version (C9600X-SUP-2)
Bengaluru 17.6.2	17.6.1r	-
Bengaluru 17.6.1	17.6.1r	-
Bengaluru 17.5.1	17.3.1r[FC2]	-
Bengaluru 17.4.1	17.3.1r[FC2]	-
Amsterdam 17.3.8a	17.3.1r[FC2]	-
Amsterdam 17.3.8	17.3.1r[FC2]	-
Amsterdam 17.3.7	17.3.1r[FC2]	-
Amsterdam 17.3.6	17.3.1r[FC2]	-
Amsterdam 17.3.5	17.3.1r[FC2]	-
Amsterdam 17.3.4	17.3.1r[FC2]	-
Amsterdam 17.3.3	17.3.1r[FC2]	-
Amsterdam 17.3.2a	17.3.1r[FC2]	-
Amsterdam 17.3.1	17.3.1r[FC2]	-
Amsterdam 17.2.1	17.1.1[FC2]	-
Amsterdam 17.1.1	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 20.

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

  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. 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 supervisor modules.
- In case of a High Availability set up, upgrade the active and standby supervisor modules.

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	
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.

Summary of Software Installation Commands	
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.

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

Caution You must comply with these cautionary guidelines during an upgrade:

- Do not power cycle the switch.
- Do not disconnect power or remove the supervisor module.
- Do not perform an online insertion and replacement (OIR) of either supervisor (in a High Availability setup), if one of the supervisor modules in the chassis is in the process of a bootloader upgrade or when the switch is booting up.
- Do not perform an OIR of a switching module (linecard) when the switch is booting up.

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

When upgrading from ...	To...
Cisco IOS XE Bengaluru 17.6.x or earlier releases	Cisco IOS XE Cupertino 17.7.x

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.

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 Fri Jul 23 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:
[switch 1]:
/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

[switch 1]:
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 Fri Jul 23 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:*.bin**

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**

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

```
Switch# show bootvar
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 =
```

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 a TFTP server or the flash , if you have copied the image to flash memory.

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

```
Switch# install add file flash:cat9k_iosxe.17.07.01.SPA.bin activate commit
_install_add_activate_commit: START Fri Jul 23 16:37:25 IST 2021

*Jul 23 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.17.07.01.SPA.bin
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

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 ---
Copying image file: flash:cat9k_iosxe.17.07.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.07.01.SPA.bin to standby
Finished initial file syncing

--- Starting Add ---
Performing Add on Active/Standby
  [R0] Add package(s) on R0
  [R0] Finished Add on R0
  [R1] Add package(s) on R1
  [R1] Finished Add on R1
Checking status of Add on [R0 R1]
Add: Passed on [R0 R1]
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
*Jul 23 16:45:21.695 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds  [R0] Activate package(s) on R0
  [R0] Finished Activate on R0
  [R1] Activate package(s) on R1
  [R1] Finished Activate on R1
Checking status of Activate on [R0 R1]
Activate: Passed on [R0 R1]
Finished Activate

*Jul 23 16:45:25.233 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R1/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds--- Starting Commit ---
Performing Commit on Active/Standby
  [R0] Commit package(s) on R0
  [R0] Finished Commit on R0
  [R1] Commit package(s) on R1
  [R1] Finished Commit on R1
Checking status of Commit on [R0 R1]
Commit: Passed on [R0 R1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Fri Jul 23 16:46:18 IST 2021
```

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:*.conf**

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

```
Switch# dir flash:*.pkg
Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104    Mar 19 2021 09:52:41 -07:00 cat9k-cc_srdriver.17.06.01.SPA.pkg
475141 -rw- 70333380   Mar 19 2021 09:52:44 -07:00 cat9k-espbase.17.06.01.SPA.pkg
475142 -rw- 13256      Mar 19 2021 09:52:44 -07:00 cat9k-guestshell.17.06.01.SPA.pkg
475143 -rw- 349635524  Mar 19 2021 09:52:54 -07:00 cat9k-rpbase.17.06.01.SPA.pkg
475149 -rw- 24248187   Mar 19 2021 09:53:02 -07:00 cat9k-rpboot.17.06.01.SPA.pkg
475144 -rw- 25285572   Mar 19 2021 09:52:55 -07:00 cat9k-sipbase.17.06.01.SPA.pkg
475145 -rw- 20947908   Mar 19 2021 09:52:55 -07:00 cat9k-sipspa.17.06.01.SPA.pkg
475146 -rw- 2962372    Mar 19 2021 09:52:56 -07:00 cat9k-srdriver.17.06.01.SPA.pkg
475147 -rw- 13284288   Mar 19 2021 09:52:56 -07:00 cat9k-webui.17.06.01.SPA.pkg
475148 -rw- 13248      Mar 19 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 (8963174400 bytes free)
```

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:/

16631  -rw- 4882 Jul 23 2021 05:39:42 +00:00  packages.conf
16634  -rw- 4882 Jul 23 2021 05:34:06 +00:00  cat9k_iosxe.17.07.01.SPA.conf
```

Step 6 Verify version

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 (fc1)
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. To perform a software image downgrade, you must be booted into IOS through **boot flash:packages.conf**.

Before you begin

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

When downgrading from ...	To ...
Cisco IOS XE Cupertino 17.7.x	Cisco IOS XE Bengaluru 17.6.x or earlier releases.

Note New switch models that are introduced in a release cannot be downgraded. The release in which a module is introduced is the minimum software version for that model. We recommend upgrading all existing hardware to the same release as the latest hardware.

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 Fri Jul 23 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  Fri Jul 23 11:42:39 IST 2021

--- 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 Jul 23 19:52:25 UTC 2019
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.17.06.01.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 23 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**

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

```
Switch# show bootvar
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 =
```

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 a TFTP server or the flash , if you have copied the image to flash memory.

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: START Fri Jul 23 21:37:25 IST 2021

*Jul 23 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.17.06.01.SPA.bin
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

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 ---
Copying image file: flash:cat9k_iosxe.17.06.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.06.01.SPA.bin to standby
Finished initial file syncing

--- Starting Add ---
Performing Add on Active/Standby
  [R0] Add package(s) on R0
  [R0] Finished Add on R0
  [R1] Add package(s) on R1
  [R1] Finished Add on R1
Checking status of Add on [R0 R1]
Add: Passed on [R0 R1]
Finished Add

Image added. Version: 17.06.1
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

--- Starting Activate ---
Performing Activate on Active/Standby

*Jul 23 21:45:21.695 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds  [R0] Activate package(s) on R0
  [R0] Finished Activate on R0
  [R1] Activate package(s) on R1
  [R1] Finished Activate on R1
Checking status of Activate on [R0 R1]
Activate: Passed on [R0 R1]
Finished Activate


*Jul 23 21:45:25.233 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R1/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds--- Starting Commit ---
Performing Commit on Active/Standby
  [R0] Commit package(s) on R0
  [R0] Finished Commit on R0
  [R1] Commit package(s) on R1
  [R1] Finished Commit on R1
Checking status of Commit on [R0 R1]
Commit: Passed on [R0 R1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Fri Jul 23 21:46:18 IST 2021
```

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) 1986-2019 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 **show firmware version all** command in IOS mode or 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 9600 Series Switches fall under these base or add-on license levels.

Base Licenses

- Network Advantage

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 Advantage

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 Gibraltar 16.11.1 to Cisco IOS XE Amsterdam 17.3.1: Smart Licensing is the default and the only supported method to manage licenses.

  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.

In the software configuration guide of the required release (17.3.x onwards), see **System Management → Smart Licensing Using Policy**.

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

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-Advantage) are ordered and fulfilled only with a perpetual or permanent license type.
- Add-on licenses (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.
- 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 9600 Series Switches datasheets at:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-series-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-series-line-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-ser-sup-eng-data-sheet-cte-en.html

Limitations and Restrictions

- Auto negotiation: The SFP+ interface (TenGigabitEthernet0/1) on the Ethernet management port with a 1G transceiver does not support auto negotiation.

- 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.
- Convergence: During SSO, a higher convergence time is observed while removing the active supervisor module installed in slot 3 of a C9606R chassis.
- Hardware Limitations — Optics:
  - Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapter —This adapter must not be installed on an even numbered port where the corresponding odd numbered port is configured as 40GE port. For example, if port 1 is configured as 40GE, CVR-QSFP-SFP10G must not be installed in port 2.

    Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapter — If you insert a 40-Gigabit Ethernet Transceiver Module to odd numbered port, the corresponding even numbered port does not work with CVR-QSFP-SFP10G adapter.
  - GLC-T and GLC-TE operating at 10/100Mbps speed are not supported with Cisco QSA Module (CVR-QSFP-SFP10G).
  - 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 — Power Supply Modules:
  - Input voltage for AC power supply modules—All AC-input power supply modules in the chassis must have the same AC-input voltage level.
  - Using power supply modules of different types—When mixing AC-input and DC-input power supplies, the AC-input voltage level must be 220 VAC.
- In-Service Software Upgrade (ISSU)
  - 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.

- 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 Cisco Catalyst 9600 Series Supervisor 2 Module, 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.

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	Description
CSCvs33050	SVL Hung - CPU HOG by Process - "Crimson Flush Transaction"
CSCvt16172	Wrong values for transceivers (DOM) in Cat9k Core switches
CSCvv91195	1 Gigabit Fiber SFPs may not link up in C9600-LC-48YL module
CSCvx87277	Cat9k may experience an unexpected reboot with Critical process fed fault on fp_0_0
CSCvx94276	%CRIMSON-3-DATABASE_MEMLEAK: Database memory leak detected in /tmp/rp/tdldb/0/IOS_PRIV_OPER_DB
CSCvy08148	Multicast packets replicates twice after redundant switch take power off
CSCvy15243	Cat9600 silent reload due to CpuCatastrophicError
CSCvy16234	IOSd crashes with system buffer pool corruption
CSCvy25845	SNMP: ifHCInOctets - snmpwalk on sub-interface octet counter does not increase
CSCvy51582	SNMP: sub-interface octet counter reports wrong value
CSCvy62453	Cat9k Switch may see Multicast traffic loss triggered by IGMP Join received on Mcast source port.

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 9600 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9600-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 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 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.