Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Amsterdam 17.1.x

First Published: 2019-11-26

Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Amsterdam 17.1.x

Introduction

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

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

Whats New in Cisco IOS XE Amsterdam 17.1.1

Hardware Features in Cisco IOS XE Amsterdam 17.1.1

Feature Name	Description and Documentation Link
Cisco QSFP to SFP or SFP+ Adapter (QSA) Module (C9300 and C9300L)	• Supported adapter module product number: CVR-QSFP-SFP10G. This module offers 10 Gigabit Ethernet and 1 Gigabit Ethernet connectivity for Quad Small Form-Factor Pluggable (QSFP)-only platforms by converting a QSFP port into an SFP or SFP+ port. • Compatible switch models: All C9300 and C9300L SKUs. • Compatible network modules: All network modules supported on the C9300 SKUs. For information about the adapter, see the Cisco QSFP to SFP or SFP+ Adapter Module Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Feature Name	Description and Documentation Link
Direct-Attach Cables for Cisco QSA Module CVR-QSFP-SFP10G (C9300 and C9300L)	Supported cable product numbers: • SFP-H10GB-ACU7M, SFP-H10GB-ACU10M • SFP-H10GB-CU1M, SFP-H10GB-CU3M, SFP-H10GB-CU5M • SFP-10G-AOC1M, SFP-10G-AOC2M, SFP-10G-AOC3M, SFP-10G-AOC5M, SFP-10G-AOC7M, SFP-10G-AOC10M For information about these cables, see Cisco 10GBASE SFP+ Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Software Features in Cisco IOS XE Amsterdam 17.1.1

Feature Name	Description, Documentation Link, and License Level Information
BIOS Protection for Golden SPI	Enables write-protection of the golden ROMMON image. See System Management → BIOS Protection. (Network Essentials and Network Advanatge)
Cisco Umbrella Integration	Provides security and policy enforcement at the Domain Name Sever (DNS) level. It enables the administrator to split the DNS traffic and directly send some of the desired DNS traffic to a specific DNS server (DNS server located within the enterprise network). See Security → Configuring Cisco Umbrella Integration. (Network Advantage)
Default Number of VTY Lines	The default number of VTY lines has changed to 32. Prior to 17.1.1, the default number of VTY lines was 16. (A license level does not apply)
ERSPAN IPv6	Introduces IPv6 support for Encapsulated Remote Switched Port Analyzer (ERSPAN). ERSPAN enables you to monitor traffic on ports or VLANs, and send the monitored traffic to destination ports. See Network Management → Configuring ERSPAN. (DNA Advantage)
Flash MIB instance retrieval count limit increase	The limitation of Flash MIB listing 100 files per partition per device has been removed. Flash MIB can now fetch all the files from the flash file system. See Network Management → Configuring Simple Network Management Protocol. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
IGMP (IPv4) : VPLS Layer 2 Snooping	Introduces support for Internet Group Management Protocol (IGMP) snooping on a Virtual Private LAN Service (VPLS) configured network. See Multiprotocol Label Switching → Configuring Virtual Private LAN Service (VPLS) and VPLS BGP-Based Autodiscovery. (Network Advantage)
Ingress and Egress Flexible Netflow on MPLS	Allows capture of IP flow information for packets undergoing Multiprotocol Label Switching (MPLS) label imposition when entering an MPLS network. These packets arrive on a device as IP packets and are transmitted as MPLS packets. Enable the feature by configuring an ingress flow monitor for IPv4 and IPv6 traffic at the customer edge (CE) facing side of the provider edge (PE) node. See Network Management → Configuring Flexible NetFlow. (DNA Essentials and DNA Advantage)
MACsec over Ethernet over MPLS (EoMPLS)	In VLAN mode, the switch (PE device) can now process packets in which the 802.1Q tag is not encrypted by the CE device. See Multiprotocol Label Switching → Configuring Ethernet-over-MPLS and Pseudowire Redundancy . (Network Advantage)
MPLS VPN InterAS Option A	MPLS VPN InterAS options provide multiple ways of interconnecting VPNs between different MPLS VPN service providers. With one of the options configured, a customer's site can exist on several carrier networks (autonomous systems) and still have seamless VPN connectivity. Of the available InterAS options, MPLS VPN InterAS Option A is the simplest to configure. This option provides back-to-back virtual routing and forwarding (VRF) connectivity (MPLS VPN providers exchange routes across VRF interfaces). See Multiprotocol Label Switching → Configuring MPLS VPN InterAS Options. (Network Advantage)
Multicast VPN Extranet Support	Enables service providers to distribute IP multicast content originating from one enterprise site to other enterprise sites. See IP Multicast Routing → Configuring Multicast VPN Extranet Support. (Network Advantage)
Neighbor Discovery (ND) Inspection Feature Deprecation	The IPv6 ND Inspection feature is deprecated. The Switch Integrated Security Features based (SISF-based) device tracking feature replaces it and offers the same capabilities. See Security → Configuring IPv6 First Hop Security. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Opening or Closing SNMP UDP Ports	A security enhancement that enables you to access the Simple Network Management Protocol (SNMP) UDP ports only after one of the requisite commands is configured. This design change secures and opens the ports only when required and prevents a device from listening to a port unnecessarily. See Network Management → Configuring Simple Network Management Protocol. (Network Essentials and Network Advantage)
Per-Port MTU Configuration	Introduces support for port level and port channel level maximum transmission unit (MTU) configuration. With Per-Port MTU configuration, you can configure different MTU values for different interfaces as well as for different port channel interfaces. See Interface and Hardware Components → Configuring Per-Port MTU. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Programmability	The following programmability features are introduced in this release: • The candidate configuration supports the confirmed commit capability. This implementation is as specified in RFC 6241 for the confirmed commit capability which, when issued, sets the running configuration to the current contents of the candidate configuration and starts a confirmed commit timer. The confirmed commit operation will be rolled back if the commit is not issued within the timeout period. The default timeout period is 600 seconds or 10 minutes. • Model-Driven Telemetry Event Notification Support: Introduces support for event notifications over the NETCONF protocol. • RESTCONF YANG-Patch Support: Introduces support for YANG-Patch media type as specified by RFC 8072. • Python 3 Support in Guest Shell: Introduces support for Python Version 3.6 is supported in Guest Shell. • TLS for gRPC Dial-Out: Introduces support for TLS for gRPC dial-out. • Cisco TrustSec uses the REST-based transport protocol for SGACL policy provisioning and data download from Cisco Identity Services Engine (ISE). The REST-based protocol is more secure, and provides reliable, and faster policy and environment data provisioning, than the RADIUS protocol that is used in previous releases. Both the REST API-based and RADIUS-based download of Cisco TrustSec data is supported. However, only one protocol can be active on a device. In Cisco IOS XE Amsterdam 17.1.1, REST-based protocol is the default. • YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1711. Some of the models introduced in this release are not backward compatible. For the complete list, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1711/BIC. Revision statements embedded in the YANG files indicate if there has been a model revision. The *README.md* file in the same GitHub location highlights changes that have been made in the release. See Programmability. (Network Essentials and Network Advantage)
VPLS Flow-Aware Transport Pseudowire Support	Provides the capability to identify individual flows within a pseudowire and provides devices the ability to use these flows to load-balance traffic. See Multiprotocol Label Switching → Configuring Virtual Private LAN Service (VPLS) and VPLS BGP-Based Autodiscovery. (Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
VPLS Protocol-Mode CLI Support	Introduces support for VPLS and VPLS BGP-based Autodiscovery configurations using protocol-CLI mode. See Multiprotocol Label Switching → Configuring Virtual Private LAN Service (VPLS) and VPLS BGP-Based Autodiscovery. (Network Advantage)

New on the Web UI	
• Cisco Umbrella Integration • New default credentials for WebUI • Power Over Ethernet (POE) • Intermediate System- Intermediate System(IS-IS) • Routing Information Protocol (RIP) • Virtual Terminal Lines (VTY)	Use the WebUI for: • Cisco Umbrella Integration—Supports integration with the cloud-based security platform–Cisco Umbrella. It provides a first line of defense by inspecting the Domain Name System (DNS) query and preventing a user from accessing a site if it is known to be malicious. Using the WebUI, the security administrator configures policies on the Cisco Umbrella Integration cloud to either allow or deny traffic towards the fully qualified domain name (FQDN). • New default credentials for WebUI—The login credentials for connecting to the device from the WebUI at Day 0 have been updated. This is available in the respective platform hardware guide. • Power Over Ethernet (POE)—The dashboard displays a dashlet for POE utilization for the switch. • Intermediate System- Intermediate System(IS-IS)—Supports Integrated Intermediate System- Intermediate System(IS-IS) routing protocol configuration for improved routing of data packets to their destination based on the best route. • Routing Information Protocol (RIP)—Supports RIP configuration for improved routing of data packets to their destination based on the hop count. • Virtual Terminal Lines (VTY)—Supports vty lines configuration in device setup, to allow a maximum number of simultaneous access to the device, remotely, through Telnet or SSH.

Important Notes

Unsupported Features

- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks

- Converged Access for Branch Deployments

- IPsec VPN

- Performance Monitoring (PerfMon)

- Virtual Routing and Forwarding (VRF)-Aware web authentication

Complete List of Supported Features

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

Accessing Hidden Commands

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

Hidden commands have always been present in Cisco IOS XE, but not equipped with CLI help. This means
that entering a question mark (?) at the system prompt does not display the list of available commands. These
commands are only meant to assist Cisco TAC in advanced troubleshooting and are not documented either.

Hidden commands are available under:

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

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

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

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

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

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

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

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

☞

Important   We recommend that you use <u>any</u> 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 9300 Series Switches—Model Numbers

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

Table 1: Cisco Catalyst 9300 Series Switches

Switch Model	Default License Level[1]	Description
C9300-24P-A	Network Advantage	Stackable 24 10/100/1000 PoE+ ports; PoE budget of 437W; 715 WAC power supply; supports StackWise-480 and StackPower
C9300-24P-E	Network Essentials	
C9300-24S-A	Network Advantage	Stackable 24 1G SFP ports; two power supply slots with 715 WAC power supply installed by default; supports StackWise-480 and StackPower.
C9300-24S-E	Network Essentials	
C9300-24T-A	Network Advantage	Stackable 24 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower
C9300-24T-E	Network Essentials	
C9300-24U-A	Network Advantage	Stackable 24 10/100/1000 UPoE ports; PoE budget of 830W; 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-24U-E	Network Essentials	
C9300-24UB-A	Network Advantage	Stackable 24 10/100/1000 Mbps UPOE ports that provide deep buffers and higher scale; PoE budget of 830W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-24UB-E	Network Essentials	
C9300-24UX-A	Network Advantage	Stackable 24 Multigigabit Ethernet 100/1000/2500/5000/10000 UPoE ports; PoE budget of 490 W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-24UX-E	Network Essentials	

Switch Model	Default License Level[1]	Description
C9300-24UXB-A	Network Advantage	Stackable 24 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports that provide deep buffers and higher scale; PoE budget of 560 W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-24UXB-E	Network Essentials	
C9300-48H-A	Network Advantage	Stackable 48 10/100/1000 Mbps UPOE+ ports; PoE budget of 822 W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-48H-E	Network Essentials	
C9300-48T-A	Network Advantage	Stackable 48 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower
C9300-48T-E	Network Essentials	
C9300-48P-A	Network Advantage	Stackable 48 10/100/1000 PoE+ ports; PoE budget of 437W; 715 WAC power supply; supports StackWise-480 and StackPower
C9300-48P-E	Network Essentials	
C9300-48S-A	Network Advantage	Stackable 48 1G SFP ports; two power supply slots with 715 WAC power supply installed by default; supports StackWise-480 and StackPower.
C9300-48S-E	Network Essentials	
C9300-48T-A	Network Advantage	Stackable 48 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower
C9300-48T-E	Network Essentials	
C9300-48U-A	Network Advantage	Stackable 48 10/100/1000 UPoE ports; PoE budget of 822 W; 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-48U-E	Network Essentials	
C9300-48UB-A	Network Advantage	Stackable 48 10/100/1000 Mbps UPOE ports that provide deep buffers and higher scale; PoE budget of 822 W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-48UB-E	Network Essentials	

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

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

Table 2: Cisco Catalyst 9300L Series Switches

Switch Model	Default License Level[2]	Description
C9300L-24T-4G-A	Network Advantage	Stackable 24x10/100/1000M Ethernet ports; 4x1G SFP fixed uplink ports; 350 WAC power supply; supports StackWise-320.
C9300L-24T-4G-E	Network Essentials	
C9300L-24P-4G-A	Network Advantage	Stackable 24x10/100/1000M PoE+ ports; 4x1G SFP fixed uplink ports; PoE budget of 505W with 715 WAC power supply; supports StackWise-320.
C9300L-24P-4G-E	Network Essentials	
C9300L-24T-4X-A	Network Advantage	Stackable 24x10/100/1000M Ethernet ports; 4x10G SFP+ fixed uplink ports; 350 WAC power supply; supports StackWise-320.
C9300L-24T-4X-E	Network Essentials	
C9300L-24P-4X-A	Network Advantage	Stackable 24x10/100/1000M PoE+ ports; 4x10G SFP+ fixed uplink ports; PoE budget of 505W with 715 WAC power supply; supports StackWise-320.
C9300L-24P-4X-E	Network Essentials	
C9300L-48T-4G-A	Network Advantage	Stackable 48x10/100/1000M Ethernet ports; 4x1G SFP fixed uplink ports; 350 WAC power supply; supports StackWise-320.
C9300L-48T-4G-E	Network Essentials	

Switch Model	Default License Level[2]	Description
C9300L-48P-4G-A	Network Advantage	Stackable 48x10/100/1000M PoE+ ports; 4x1G SFP fixed uplink ports; PoE budget of 505W with 715 WAC power supply; supports StackWise-320.
C9300L-48P-4G-E	Network Essentials	
C9300L-48T-4X-A	Network Advantage	Stackable 48x10/100/1000M Ethernet ports; 4x10G SFP+ fixed uplink ports; 350 WAC power supply; supports StackWise-320.
C9300L-48T-4X-E	Network Essentials	
C9300L-48P-4X-A	Network Advantage	Stackable 48x10/100/1000M PoE+ ports; 4x10G SFP+ fixed uplink ports; PoE budget of 505W with 715 WAC power supply; supports StackWise-320.
C9300L-48P-4X-E	Network Essentials	
C9300L-48PF-4G-A	Network Advantage	Stackable 48 10/100/1000 Mbps PoE+ ports; 4x1G SFP+ fixed uplink ports; PoE budget of 890 W with 1100 WAC power supply; supports StackWise-320.
C9300L-48PF-4G-E	Network Essentials	
C9300L-48PF-4X-A	Network Advantage	Stackable 48 10/100/1000 Mbps PoE+ ports; 4x10G SFP+ fixed uplink ports; PoE budget of 890 W with 1100 WAC power supply; supports StackWise-320.
C9300L-48PF-4X-E	Network Essentials	
C9300L-24UXG-4X-A	Network Advantage	Stackable 16 10/100/1000 Mbps and 8 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 4x10G SFP+ fixed uplink ports; PoE budget of 880 W with 1100 WAC power supply; supports StackWise-320.
C9300L-24UXG-4X-E	Network Essentials	
C9300L-24UXG-2Q-A	Network Advantage	Stackable 16 10/100/1000 Mbps and 8 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 2x40G QSFP+ fixed uplink ports; PoE budget of 722 W with 1100 WAC power supply; supports StackWise-320.
C9300L-24UXG-2Q-E	Network Essentials	
C9300L-48UXG-4X-A	Network Advantage	Stackable 36 10/100/1000 Mbps and 12 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 4x10G SFP+ fixed uplink ports; PoE budget of 675 W with 1100 WAC power supply; supports StackWise-320.
C9300L-48UXG-4X-E	Network Essentials	

Switch Model	Default License Level[2]	Description
C9300L-48UXG-2Q-A	Network Advantage	Stackable 36 10/100/1000 Mbps and 12 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 2x40G QSFP+ fixed uplink ports; PoE budget of 675 W with 1100 WAC power supply; supports StackWise-320.
C9300L-48UXG-2Q-E	Network Essentials	

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

Network Modules

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

Network Module	Description
C3850-NM-4-1G [1]	Four 1 Gigabit Ethernet SFP module slots
C3850-NM-2-10G [1]	Two 10 Gigabit Ethernet SFP module slots
C3850-NM-4-10G [1]	Four 10 Gigabit Ethernet SFP module slots
C3850-NM-8-10G [1]	Eight 10 Gigabit Ethernet SFP module slots
C3850-NM-2-40G [1]	Two 40 Gigabit Ethernet SFP module slots
C9300-NM-4G [2]	Four 1 Gigabit Ethernet SFP module slots
C9300-NM-4M [2]	Four MultiGigabit Ethernet slots
C9300-NM-8X [2]	Eight 10 Gigabit Ethernet SFP+ module slots
C9300-NM-2Q [2]	Two 40 Gigabit Ethernet QSFP+ module slots
C9300-NM-2Y [2]	Two 25 Gigabit Ethernet SFP28 module slots

Note

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

2. These network modules are supported only on the C9300 SKUs of the Cisco Catalyst 9300 Series Switches.

The following table lists the network modules that are supported on the Cisco Catalyst 9300X-HXN Series Switches and the ports that are usable on each of these network module:

Table 3: Network Modules Supported on Catalyst 9300X-HXN Series Switches

Network Module	Cisco IOS XE Cupertino 17.7.1 and Previous Releases	Cisco IOS XE Cupertino 17.8.1 and Later Releases
C9300X-NM-8Y (8x25G)	Ports 1 to 4 usable.	Ports 1 to 6 usable. Ports 7 and 8 are permanently disabled.
C9300X-NM-8M (8xmGig)	Ports 1 to 4 usable.	Ports 1 to 6 usable. Ports 7 and 8 are permanently disabled.
C9300X-NM-2C (2x100G/2x40G)	Ports 1 to 2 usable. No breakout cable support.	Ports 1 and 2 usable. Breakout cable supported only on port 1. No support for breakout cable on port 2.

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 9300 Series Switches, Cisco Identity Services Engine, Cisco Access Control Server, and Cisco Prime Infrastructure.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Amsterdam 17.1.1	2.7	-	C9300: PI 3.6 + PI 3.6 latest maintenance release + PI 3.6 latest device pack C9300L: - See Cisco Prime Infrastructure 3.6 → **Downloads**.
Gibraltar 16.12.8	2.6	-	C9300: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack C9300L: - See Cisco Prime Infrastructure 3.9 → Downloads.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.12.7	2.6	-	C9300: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack C9300L: - See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.6	2.6	-	C9300: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack C9300L: - See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.5b	2.6	-	C9300: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack C9300L: - See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.5	2.6	-	C9300: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack C9300L: - See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.4	2.6	-	C9300: PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack C9300L: - See Cisco Prime Infrastructure 3.8 → Downloads.
Gibraltar 16.12.3a	2.6	-	C9300: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack C9300L: - See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.3	2.6	-	C9300: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack C9300L: - See Cisco Prime Infrastructure 3.5 → **Downloads**.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.12.2	2.6	-	C9300: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack C9300L: - See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.1	2.6	-	C9300: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack C9300L: - 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**.
Fuji 16.9.8	2.5 2.1	5.4 5.5	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.7	2.5 2.1	5.4 5.5	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.6	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.5	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.

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

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

Web UI System Requirements

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

Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[3]	512 MB[4]	256	1280 x 800 or higher	Small

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

Software Requirements

Operating Systems

- Windows 10 or later

- Mac OS X 10.9.5 or later

Browsers

- Google Chrome—Version 59 or later (On Windows and Mac)

- Microsoft Edge

- Mozilla Firefox—Version 54 or later (On Windows and Mac)

- Safari—Version 10 or later (On Mac)

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.

Release	ROMMON Version (C9300 Models)	ROMMON Version (C9300L Models)	ROMMON Version (C9300X Models)	ROMMON Version (C9300LM Models)
Amsterdam 17.1.1	17.1.1r [FC1]	17.1.1r [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 Amsterdam 17.1.1	CAT9K_IOSXE	cat9k_iosxe.17.01.01.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.01.01.SPA

Upgrading the ROMMON

To know the ROMMON or bootloader version that applies to every major and maintenance release, see ROMMON Versions, on page 17.

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 when you boot up your switch with the new image for the first time.

• 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 switch stack, perform the upgrade on the active switch and all members of the stack.

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.

Automatic Microcode Upgrade

During a Cisco IOS image upgrade or downgrade on a PoE or UPoE switch, microcode is upgraded to reflect applicable feature enhancements and bug fixes. A microcode upgrade occurs only during an image upgrade or downgrade, on PoE or UPoE switches. It does not occur during switch reloads or on non-PoE switches.

Depending on the release you are upgrading from, microcode upgrade can occur during the install operation or during bootup:

• If the release you are upgrading *from* does not support microcode updates during the course of installation, microcode is updated during boot up, and an additional 4 minutes (approximately) are required to complete the microcode upgrade, in addition to the normal reload time. Data traffic is not forwarded when microcode is upgraded during bootup.

• When using **install** commands to upgrade, microcode is upgraded during the install operation, and no additional time is required during bootup. Here microcode is updated before the reload that occurs as part of the image upgrade process. Data traffic continues to be forwarded during the upgrade.

Do not restart the switch during the upgrade or downgrade process.

The following console messages are displayed during microcode upgrade.

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

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

Front-end Microcode IMG MGR: Preparing to program device microcode...
Front-end Microcode IMG MGR: Preparing to program device[0], index=0 ...594412 bytes....
Skipped[0].
Front-end Microcode IMG MGR: Preparing to program device[0], index=1 ...393734 bytes.
Front-end Microcode IMG MGR: Programming device 0...rwRrrrrrw..
0%.................................................................
10%................................................................
20%.................................................................
30%................................................................
```

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

Software Installation Commands

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

✎

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

Summary of request platform software Commands	
Device# **request platform software package ?**	
clean	Cleans unnecessary package files from media
copy	Copies package to media
describe	Describes package content

Summary of request platform software Commands	
expand	Expands all-in-one package to media
install	Installs the package
uninstall	Uninstalls the package
verify	Verifies In Service Software Upgrade (ISSU) software package compatibility

Upgrading in Install Mode

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

Before you begin

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

When upgrading from ...	Use these commands...	To upgrade to...
Cisco IOS XE Everest 16.5.1a or Cisco IOS XE Everest 16.6.1	Only **request platform software** commands	Cisco IOS XE Amsterdam 17.1.1
Cisco IOS XE Everest 16.6.2 and later	Either **install** commands or **request platform software** commands	

The sample output in this section displays upgrade from

- Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Amsterdam 17.1.1 using **request platform software** commands.

- Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Amsterdam 17.1.1 using **install** commands.

Procedure

Step 1 Clean Up

Ensure that you have at least 1GB of space in flash to expand a new image. Clean up old installation files in case of insufficient space.

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

The following sample output displays the cleaning up of unused files, by using the **request platform software package clean** command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Amsterdam 17.1.1. Use the **switch all** option to clean up all the switches in your stack

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

```
Switch# request platform software package clean switch all
Running command on switch 1
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.
done.

Running command on switch 2
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.

Running command on switch 3
Cleaning up unnecessary package files
```

```
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
hexdump: NVRAM: No such file or directory
hexdump: all input file arguments failed
head: cannot open 'NVRAM' for reading: No such file or directory
NVRAM: No such file or directory
hexdump: NVRAM: No such file or directory
hexdump: stdin: Bad file descriptor
tail: cannot open 'NVRAM' for reading: No such file or directory
hexdump: NVRAM: No such file or directory
hexdump: all input file arguments failed
cat9k-cc_srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.

The following files will be deleted:
[1]:
/flash/cat9k-cc_srdriver.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-
[2]:
/flash/cat9k-cc_srdriver.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-
[3]:
/flash/cat9k-cc_srdriver.SPA.pkg
```

```
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-

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

The following sample output displays the cleaning up of unused files, by using the **install remove inactive**
command, for upgrade scenario Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Amsterdam 17.1.1:

```
Switch# install remove inactive
install_remove: START Thu Nov 20 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.
The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.16.12.01.SPA.pkg
```

```
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-guestshell.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
/flash/cat9k-webui.16.12.01.SPA.pkg
/flash/cat9k-wlc.16.12.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.12.01.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 Thu Nov 20 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.17.01.01.SPA.bin flash:
destination filename [cat9k_iosxe.17.01.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.17.01.01.SPA.bin...
Loading /cat9k_iosxe.17.01.01.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 Nov 20 2019 10:18:11 -07:00 cat9k_iosxe.17.01.01.SPA.bin
```

```
        11353194496 bytes total (8976625664 bytes free)
```

Step 3   Set boot variable

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

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

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

b) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

c) **show boot system**

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

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

```
Switch# show boot system
```

Step 4   Software install image to flash

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

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

```
Switch# request platform software package install switch all file
flash-3:cat9k_iosxe.17.01.01.SPA.bin auto-copy.
```

The following sample output displays installation of the Cisco IOS XE Amsterdam 17.1.1 software image to flash, by using the **request platform software package install** command, for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Amsterdam 17.1.1.

```
Switch# request platform software package install switch all file
flash:cat9k_iosxe.17.01.01.SPA.bin auto-copy

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

Expanding image file: flash:cat9k_iosxe.17.01.01.SPA.bin
[1]: Copying flash:cat9k_iosxe.17.01.01.SPA.bin from switch 1 to switch 2 3
[2 3]: Finished copying to switch 2 3
[1 2 3]: Expanding file
[1 2 3]: Finished expanding all-in-one software package in switch 1 2 3
SUCCESS: Finished expanding all-in-one software package.
[1 2 3]: Performing install
SUCCESS: install finished
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
```

```
                  Removed cat9k-sipbase.16.05.01a.SPA.pkg
                  Removed cat9k-sipspa.16.05.01a.SPA.pkg
                  Removed cat9k-srdriver.16.05.01a.SPA.pkg
                  Removed cat9k-webui.16.05.01a.SPA.pkg
                  Removed cat9k-wlc.16.05.01a.SPA.pkg
                  New files list:
                  Added cat9k-cc_srdriver.17.01.01.SPA.pkg
                  Added cat9k-espbase.17.01.01.SPA.pkg
                  Added cat9k-guestshell.17.01.01.SPA.pkg
                  Added cat9k-rpbase.17.01.01.SPA.pkg
                  Added cat9k-rpboot.17.01.01.SPA.pkg
                  Added cat9k-sipbase.17.01.01.SPA.pkg
                  Added cat9k-sipspa.17.01.01.SPA.pkg
                  Added cat9k-srdriver.17.01.01.SPA.pkg
                  Added cat9k-webui.17.01.01.SPA.pkg
                  Added cat9k-wlc.17.01.01.SPA.pkg
                  Finished list of software package changes
                  SUCCESS: Software provisioned. New software will load on reboot.
                  [1]: Finished install successful on switch 1
                  [2]: install package(s) on switch 2
                  --- Starting list of software package changes ---
                  Old files list:
                  Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
                  Removed cat9k-espbase.16.05.01a.SPA.pkg
                  Removed cat9k-guestshell.16.05.01a.SPA.pkg
                  Removed cat9k-rpbase.16.05.01a.SPA.pkg
                  Removed cat9k-rpboot.16.05.01a.SPA.pkg
                  Removed cat9k-sipbase.16.05.01a.SPA.pkg
                  Removed cat9k-sipspa.16.05.01a.SPA.pkg
                  Removed cat9k-srdriver.16.05.01a.SPA.pkg
                  Removed cat9k-webui.16.05.01a.SPA.pkg
                  Removed cat9k-wlc.16.05.01a.SPA.pkg
                  New files list:
                  Added cat9k-cc_srdriver.17.01.01.SPA.pkg
                  Added cat9k-espbase.17.01.01.SPA.pkg
                  Added cat9k-guestshell.17.01.01.SPA.pkg
                  Added cat9k-rpbase.17.01.01.SPA.pkg
                  Added cat9k-rpboot.17.01.01.SPA.pkg
                  Added cat9k-sipbase.17.01.01.SPA.pkg
                  Added cat9k-sipspa.17.01.01.SPA.pkg
                  Added cat9k-srdriver.17.01.01.SPA.pkg
                  Added cat9k-webui.17.01.01.SPA.pkg
                  Added cat9k-wlc.17.01.01.SPA.pkg
                  Finished list of software package changes
                  SUCCESS: Software provisioned. New software will load on reboot.
                  [2]: Finished install successful on switch 2
                  [3]: install package(s) on switch 3
                  --- Starting list of software package changes ---
                  Old files list:
                  Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
                  Removed cat9k-espbase.16.05.01a.SPA.pkg
                  Removed cat9k-guestshell.16.05.01a.SPA.pkg
                  Removed cat9k-rpbase.16.05.01a.SPA.pkg
                  Removed cat9k-rpboot.16.05.01a.SPA.pkg
                  Removed cat9k-sipbase.16.05.01a.SPA.pkg
                  Removed cat9k-sipspa.16.05.01a.SPA.pkg
                  Removed cat9k-srdriver.16.05.01a.SPA.pkg
                  Removed cat9k-webui.16.05.01a.SPA.pkg
                  Removed cat9k-wlc.16.05.01a.SPA.pkg
                  New files list:
                  Added cat9k-cc_srdriver.17.01.01.SPA.pkg
                  Added cat9k-espbase.17.01.01.SPA.pkg
                  Added cat9k-guestshell.17.01.01.SPA.pkg
                  Added cat9k-rpbase.17.01.01.SPA.pkg
```

```
Added cat9k-rpboot.17.01.01.SPA.pkg
Added cat9k-sipbase.17.01.01.SPA.pkg
Added cat9k-sipspa.17.01.01.SPA.pkg
Added cat9k-srdriver.17.01.01.SPA.pkg
Added cat9k-webui.17.01.01.SPA.pkg
Added cat9k-wlc.17.01.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[3]: Finished install successful on switch 3
Checking status of install on [1 2 3]
[1 2 3]: Finished install in switch 1 2 3
SUCCESS: Finished install: Success on [1 2 3]
```

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

The following sample output displays installation of the Cisco IOS XE Amsterdam 17.1.1 software image to flash, by using the **install add file activate commit** command, for upgrade scenario Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Amsterdam 17.1.1:

```
Switch# install add file flash:cat9k_iosxe.17.01.01.SPA.bin activate commit

install_add_activate_commit: START Thu Nov 20 19:54:51 UTC 2018

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

[OK]Modified configuration has been saved

*Nov 20 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Nov 20 19:54:55 install_engine.sh:

%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.17.01.01.SPA.bininstall_add_activate_commit: Adding PACKAGE

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

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.17.01.01.SPA.bin to the selected switch(es)
Finished initial file syncing

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

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.01.01.SPA.pkg
/flash/cat9k-webui.17.01.01.SPA.pkg
/flash/cat9k-srdriver.17.01.01.SPA.pkg
/flash/cat9k-sipspa.17.01.01.SPA.pkg
/flash/cat9k-sipbase.17.01.01.SPA.pkg
/flash/cat9k-rpboot.17.01.01.SPA.pkg
/flash/cat9k-rpbase.17.01.01.SPA.pkg
/flash/cat9k-guestshell.17.01.01.SPA.pkg
/flash/cat9k-espbase.17.01.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.01.01.SPA.pkg
```

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

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

*Nov 20 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: nov 20 19:57:41 rollback_timer.sh:

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

Install will reload the system now!
SUCCESS: install_add_activate_commit Thu Nov 20 19:57:48 UTC 2019
Switch#
```

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

Step 5   **dir flash:**

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

The following is sample output of the **dir flash:** command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Amsterdam 17.1.1:

```
Switch# dir flash:*.pkg

Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104   Jul 31 2019 09:52:41 -07:00 cat9k-cc_srdriver.16.05.01a.SPA.pkg
475141 -rw- 70333380  Jul 31 2019 09:52:44 -07:00 cat9k-espbase.16.05.01a.SPA.pkg
475142 -rw- 13256     Jul 31 2019 09:52:44 -07:00 cat9k-guestshell.16.05.01a.SPA.pkg
475143 -rw- 349635524 Jul 31 2019 09:52:54 -07:00 cat9k-rpbase.16.05.01a.SPA.pkg
475149 -rw- 24248187  Jul 31 2019 09:53:02 -07:00 cat9k-rpboot.16.05.01a.SPA.pkg
475144 -rw- 25285572  Jul 31 2019 09:52:55 -07:00 cat9k-sipbase.16.05.01a.SPA.pkg
475145 -rw- 20947908  Jul 31 2019 09:52:55 -07:00 cat9k-sipspa.16.05.01a.SPA.pkg
475146 -rw- 2962372   Jul 31 2019 09:52:56 -07:00 cat9k-srdriver.16.05.01a.SPA.pkg
475147 -rw- 13284288  Jul 31 2019 09:52:56 -07:00 cat9k-webui.16.05.01a.SPA.pkg
475148 -rw- 13248     Jul 31 2019 09:52:56 -07:00 cat9k-wlc.16.05.01a.SPA.pkg

491524 -rw- 25711568  Nov 20 2019 11:49:33 -07:00 cat9k-cc_srdriver.17.01.01.SPA.pkg
491525 -rw- 78484428  Nov 20 2019 11:49:35 -07:00 cat9k-espbase.17.01.01.SPA.pkg
491526 -rw- 1598412   Nov 20 2019 11:49:35 -07:00 cat9k-guestshell.17.01.01.SPA.pkg
491527 -rw- 404153288 Nov 20 2019 11:49:47 -07:00 cat9k-rpbase.17.01.01.SPA.pkg
491533 -rw- 31657374  Nov 20 2019 11:50:09 -07:00 cat9k-rpboot.17.01.01.SPA.pkg
491528 -rw- 27681740  Nov 20 2019 11:49:48 -07:00 cat9k-sipbase.17.01.01.SPA.pkg
491529 -rw- 52224968  Nov 20 2019 11:49:49 -07:00 cat9k-sipspa.17.01.01.SPA.pkg
491530 -rw- 31130572  Nov 20 2019 11:49:50 -07:00 cat9k-srdriver.17.01.01.SPA.pkg
491531 -rw- 14783432  Nov 20 2019 11:49:51 -07:00 cat9k-webui.17.01.01.SPA.pkg
491532 -rw- 9160      Nov 20 2019 11:49:51 -07:00 cat9k-wlc.17.01.01.SPA.pkg
```

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

The following is sample output of the **dir flash:** command for the Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Amsterdam 17.1.1 upgrade scenario:

```
Switch# dir flash:*.pkg

Directory of flash:/
475140 -rw- 2012104   Jul 31 2019 09:52:41 -07:00 cat9k-cc_srdriver.16.12.01.SPA.pkg
475141 -rw- 70333380  Jul 31 2019 09:52:44 -07:00 cat9k-espbase.16.12.01.SPA.pkg
475142 -rw- 13256     Jul 31 2019 09:52:44 -07:00 cat9k-guestshell.16.12.01.SPA.pkg
475143 -rw- 349635524 Jul 31 2019 09:52:54 -07:00 cat9k-rpbase.16.12.01.SPA.pkg
475149 -rw- 24248187  Jul 31 2019 09:53:02 -07:00 cat9k-rpboot.16.12.01.SPA.pkg
475144 -rw- 25285572  Jul 31 2019 09:52:55 -07:00 cat9k-sipbase.16.12.01.SPA.pkg
475145 -rw- 20947908  Jul 31 2019 09:52:55 -07:00 cat9k-sipspa.16.12.01.SPA.pkg
475146 -rw- 2962372   Jul 31 2019 09:52:56 -07:00 cat9k-srdriver.16.12.01.SPA.pkg
475147 -rw- 13284288  Jul 31 2019 09:52:56 -07:00 cat9k-webui.16.12.01.SPA.pkg
475148 -rw- 13248     Jul 31 2019 09:52:56 -07:00 cat9k-wlc.16.12.01.SPA.pkg

491524 -rw- 25711568  Nov 20 2019 11:49:33 -07:00 cat9k-cc_srdriver.17.01.01.SPA.pkg
491525 -rw- 78484428  Nov 20 2019 11:49:35 -07:00 cat9k-espbase.17.01.01.SPA.pkg
491526 -rw- 1598412   Nov 20 2019 11:49:35 -07:00 cat9k-guestshell.17.01.01.SPA.pkg
491527 -rw- 404153288 Nov 20 2019 11:49:47 -07:00 cat9k-rpbase.17.01.01.SPA.pkg
491533 -rw- 31657374  Nov 20 2019 11:50:09 -07:00 cat9k-rpboot.17.01.01.SPA.pkg
491528 -rw- 27681740  Nov 20 2019 11:49:48 -07:00 cat9k-sipbase.17.01.01.SPA.pkg
491529 -rw- 52224968  Nov 20 2019 11:49:49 -07:00 cat9k-sipspa.17.01.01.SPA.pkg
491530 -rw- 31130572  Nov 20 2019 11:49:50 -07:00 cat9k-srdriver.17.01.01.SPA.pkg
491531 -rw- 14783432  Nov 20 2019 11:49:51 -07:00 cat9k-webui.17.01.01.SPA.pkg
491532 -rw- 9160      Nov 20 2019 11:49:51 -07:00 cat9k-wlc.17.01.01.SPA.pkg
11353194496 bytes total (9544245248 bytes free)
Switch#
```

The following sample output 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.17.01.01.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 Nov 20 2019 10:59:16 -07:00 packages.conf
516098 -rw- 7406 Nov 20 2019 10:58:08 -07:00 cat9k_iosxe.17.01.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

Step 6   **upgrade rom-monitor capsule golden switch** [*number*] **R0**

Use this command to upgrade the ROMMON version. After you enter the command, confirm upgrade at the system prompt.

For more information about this, see Upgrading the ROMMON, on page 18 in this document.

```
Switch# upgrade rom-monitor capsule golden switch active R0
This operation will reload the switch and take a few minutes to complete. Do you want to
proceed (y/n)? [confirm]y
Switch#
Initializing Hardware...
<output truncated>
```

Step 7 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

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

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

c) **show version**

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

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

The following sample output of the **show version** command displays the Cisco IOS XE Gibraltar 16.12.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.01.01
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.1.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Sat 09-Nov-19 10:39 by mcpre
<output truncated>
```

Downgrading in Install Mode

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

Before you begin

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

When downgrading from ...	Use these commands...	To downgrade to...
Cisco IOS XE Amsterdam 17.1.1	Either **install** commands or **request platform software** commands	Cisco IOS XE Gibraltar 16.12.x or earlier releases

Starting from Cisco IOS XE Gibraltar 16.12.1, a new microcode is introduced to support IEEE 802.3bt Type 3 standard for UPOE switches in the series (C9300-24U, C9300-48U, C9300-24UX, C9300-48UXM, C9300-48UN). The new microcode is not backward-compatible with some releases, because of which you must also downgrade the microcode when you downgrade to one of these releases. If the microcode is not downgraded, PoE features will be impacted after the downgrade.

Depending on the release you are downgrading to and the commands you use to downgrade, review the table below for the action you may have to take:

When downgrading from ...	To one of These Releases	by Using...	Action For Microcode Downgrade
Cisco IOS XE Gibraltar 16.12.1 or a later release	Cisco IOS XE Everest 16.6.1 through Cisco IOS XE Everest 16.6.6	**install** commands	Microcode will roll back automatically as part of the software installation. No further action is required.
	Cisco IOS XE Fuji 16.9.1 through Cisco IOS XE Fuji 16.9.2	**request platform software** commands or or bundle boot	Manually downgrade the microcode before downgrading the software image. Enter the **hw-module mcu rollback** command in global configuration mode, to downgrade microcode.

The sample output in this section shows downgrade from Cisco IOS XE Amsterdam 17.1.1 to Cisco IOS XE Gibraltar 16.12.1, by using the **install** commands.

☞

Important   The release in which a switch model is introduced is the minimum software version for that model. New switch models that are introduced in a release cannot be downgraded. If you add a new switch model to an existing stack, we recommend upgrading all existing switches to the latest release.

Procedure

Step 1   Clean Up

Ensure that you have at least 1GB of space in flash to expand a new image. Clean up old installation files in case of insufficient space.

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

The following sample output displays the cleaning up of Cisco IOS XE Gibraltar 16.12.1 files using the **install remove inactive** command:

```
Switch# install remove inactive

install_remove: START Mon Jul 22 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.17.01.01.SPA.pkg
/flash/cat9k-espbase.17.01.01.SPA.pkg
/flash/cat9k-guestshell.17.01.01.SPA.pkg
/flash/cat9k-rpbase.17.01.01.SPA.pkg
/flash/cat9k-rpboot.17.01.01.SPA.pkg
/flash/cat9k-sipbase.17.01.01.SPA.pkg
```

```
/flash/cat9k-sipspa.17.01.01.SPA.pkg
/flash/cat9k-srdriver.17.01.01.SPA.pkg
/flash/cat9k-webui.17.01.01.SPA.pkg
/flash/cat9k-wlc.17.01.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.17.01.01.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 Mon Jul 22 19:52:25 UTC 2019
Switch#
```

Step 2   Copy new image to flash

a)   **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.12.01.SPA.bin flash:
Destination filename [cat9k_iosxe.16.12.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.12.01.SPA.bin...
Loading /cat9k_iosxe.16.12.01.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 22 2018 13:35:16 -07:00 cat9k_iosxe.16.12.01.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3   Downgrade software image

• **install add file activate commit**

- **request platform software package install**

The following example displays the installation of the Cisco IOS XE Gibraltar 16.12.1 software image to flash with microcode downgrade, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.16.12.01.SPA.bin activate commit

install_add_activate_commit: START Thu Nov 14 23:51:14 UTC 2019
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.12.01.SPA.bin to the selected switch(es)
Finished initial file syncing

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

Image added. Version: 16.6.1.0.202
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-webui.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-guestshell.16.12.01.SPA.pkg
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.12.01.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on all members
[1] Activate package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
Removed cat9k-cc_srdriver.17.01.01.SPA.pkg
Removed cat9k-espbase.17.01.01.SPA.pkg
Removed cat9k-guestshell.17.01.01.SPA.pkg
Removed cat9k-rpbase.17.01.01.SPA.pkg
Removed cat9k-rpboot.17.01.01.SPA.pkg
Removed cat9k-sipbase.17.01.01.SPA.pkg
Removed cat9k-sipspa.17.01.01.SPA.pkg
Removed cat9k-srdriver.17.01.01.SPA.pkg
Removed cat9k-webui.17.01.01.SPA.pkg
Removed cat9k-wlc.17.01.01.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.12.01.SPA.pkg
Added cat9k-espbase.16.12.01.SPA.pkg
Added cat9k-guestshell.16.12.01.SPA.pkg
Added cat9k-rpbase.16.12.01.SPA.pkg
Added cat9k-rpboot.16.12.01.SPA.pkg
Added cat9k-sipbase.16.12.01.SPA.pkg
Added cat9k-sipspa.16.12.01.SPA.pkg
Added cat9k-srdriver.16.12.01.SPA.pkg
Added cat9k-webui.16.12.01.SPA.pkg
Finished list of software package changes
[1] Finished Activate on switch 1
```

```
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

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

[1]: Performing Upgrade_Service
%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (local/local): Starting boot preupgrade
300+0 records in
300+0 records out
307200 bytes (307 kB, 300 KiB) copied, 0.315648 s, 973 kB/s
/tmp/microcode_update/boot_pkg/nyquist/usr/platform/polaris_adelphi_rommon_sb.bin: No such
 file or directory
MM [1] MCU version 127 sw ver 172
MM [2] MCU version 127 sw ver 172


MCU UPGRADE IN PROGRESS... PLEASE DO NOT POWER CYCLE!!

Front-end Microcode IMG MGR: found 4 microcode images for 1 device.
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_0 update needed: no
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_1 update needed: yes
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_2 update needed: yes
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_3 update needed: no

Front-end Microcode IMG MGR: Preparing to program device microcode...
Front-end Microcode IMG MGR: Preparing to program device[0], index=0 ...594412 bytes....
Skipped[0].
Front-end Microcode IMG MGR: Preparing to program device[0], index=1 ...409334 bytes.
Front-end Microcode IMG MGR: Programming device
0...rw..0%....10%....20%....30%...40%....50%....60%....70%...80%....90%....100%
Front-end Microcode IMG MGR: Preparing to program device[0], index=2 ...25210 bytes.
Front-end Microcode IMG MGR: Programming device
0...rrrrrw..0%....10%....20%......30%...40%......50%....60%......70%...80%......90%....100%w

% Front-end Microcode IMG download pre-reload on sub=0
Front-end Microcode IMG MGR: Preparing to program device[0], index=3 ...90974 bytes....
Skipped[3].
Front-end Microcode IMG MGR: Microcode programming complete in 263 seconds


MCU UPGRADE COMPLETED!!... SUCCESS: Upgrade_Service finished
Install will reload the system now!
SUCCESS: install_add_activate_commit Thu Nov 14 23:59:48 UTC 2019
Switch#
```

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

Step 4   Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

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

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

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

c) **show version**

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

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

The following sample output of the **show version** command displays the Cisco IOS XE Gibraltar 16.12.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.12.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.12.1, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 20-Nov-19 19:26 by mcpre
<output truncated>
```

Licensing

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

License Levels

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

Base Licenses

- Network Essentials

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

Add-On Licenses

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

- DNA Essentials

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

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

License Types

The following license types are available:

• Permanent—for a license level, and without an expiration date.

• Term—for a license level, and for a three, five, or seven year period.

• Evaluation—a license that is not registered.

License Levels - Usage Guidelines

• Base licenses (Network Essentials and Network-Advantage) are ordered and fulfilled only with a permanent license type.

• Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a term license type.

• An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.

• When ordering an add-on license with a base license, note the combinations that are permitted and those that are not permitted:

Table 4: Permitted Combinations

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

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

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

Cisco Smart Licensing

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

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).

- Unified Management: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.

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

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

☞

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

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

Deploying Smart Licensing

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

Procedure

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

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

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

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

Step 3   Complete the Cisco Smart Software Manager set up.

a)   Accept the Smart Software Licensing Agreement.

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

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

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

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

With this,

- The device is now in an authorized state and ready to use.

• The licenses that you have purchased are displayed in your Smart Account.

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

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

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

How Upgrading or Downgrading Software Affects Smart Licensing

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

☞

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

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

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

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

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

Scaling Guidelines

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

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

Limitations and Restrictions

• 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 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.

• QoS restrictions

  • When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.

  • For QoS policies, only switched virtual interfaces (SVI) are supported for logical interfaces.

  • QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.

  • Stack Queuing and Scheduling (SQS) drops CPU bound packets exceeding 1.4 Gbps.

• Secure Shell (SSH)

  • Use SSH Version 2. SSH Version 1 is not supported.

  • When the device is running SCP and SSH cryptographic operations, expect high CPU until the SCP read process is completed. SCP supports file transfers between hosts on a network and uses SSH for the transfer.

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

• Stacking:

  • A switch stack supports up to eight stack members.

  • Only homogenous stacking is supported, mixed stacking is not.

    C9300 SKUs can be stacked only with other C9300 SKUs. Similarly C9300L SKUs can be stacked only with other C9300L SKUs.

    The following additional restriction applies to the C9300-24UB, C9300-24UXB, and C9300-48UB models of the series: These models can be stacked only with each other. They cannot be stacked with other C9300 SKUs.

  • Auto upgrade for a new member switch is supported only in the install mode.

• 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
```

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

- Wired Application Visibility and Control limitations:

  - NBAR2 (QoS and Protocol-discovery) configuration is allowed only on wired physical ports. It is not supported on virtual interfaces, for example, VLAN, port channel nor other logical interfaces.

  - NBAR2 based match criteria 'match protocol' is allowed only with marking or policing actions. NBAR2 match criteria will not be allowed in a policy that has queuing features configured.

  - 'Match Protocol': up to 256 concurrent different protocols in all policies.

  - NBAR2 and Legacy NetFlow cannot be configured together at the same time on the same interface. However, NBAR2 and wired AVC Flexible NetFlow can be configured together on the same interface.

  - Only IPv4 unicast (TCP/UDP) is supported.

  - AVC is not supported on management port (Gig 0/0)

  - NBAR2 attachment should be done only on physical access ports. Uplink can be attached as long as it is a single uplink and is not part of a port channel.

  - Performance—Each switch member is able to handle 2000 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.

  - Scale—Able to handle up to 20000 bi-directional flows per 24 access ports and per 48 access ports.

- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.

- Embedded Event Manager—Identity event detector is not supported on Embedded Event Manager.

- 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 Amsterdam 17.1.x

Identifier	Description
CSCvq72472	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvr87767	PDs not detected and powered up on 9300 with 2-pair cables
CSCvr88090	Cat9300 crash on running show platform software fed switch 1 fss abstraction
CSCvr92287	EPC with packet-len opt breaks CPU in-band path for bigger frames
CSCvr92660	STP BPDUs not being sent from FED to IOSd
CSCvr98281	After valid ip conflict, SVI admin down responds to GARP
CSCvr98683	During repeated reload test one of the switch members in a stack may takes more time to come up
CSCvr99132	SPANed multicast packet reduced TTL
CSCvs14893	802.1x-MultiAuth/MultiDomain: C9K - Traffic drop in egress direction for Data-Vlan on a Auth port
CSCvu13029	Intermittent Link Flaps on mGig Cat9300 switches to mGig capable endpoints

Resolved Caveats in Cisco IOS XE Amsterdam 17.1.1

Identifier	Description
CSCvo66246	Enabling SPAN source of VLAN 1 affects LACP operations
CSCvp37420	40GE Uplink does not come up after reload or switchover
CSCvp37771	9300 Mgig - Half-Pair Ethernet Cables do not auto-negotiate to 100 Full with Certain IP Phones
CSCvp70112	EnvMon trap not received after Power Supply and FAN OIR
CSCvp84502	ERSPAN destination does not work or forward traffic
CSCvq05337	Cat9500 || v169_3_hemit_es_throttle ES image || EGR_INVALID_REWRITE counter increasing in mVPN setup
CSCvq22224	cat9k // evpn/vxlan // dhcp relay not working over l3vni
CSCvq29115	Failed to get Board ID shown if stack member boots up
CSCvq30460	SYS-2-BADSHARE: Bad refcount in datagram_done - messages seen during system churn
CSCvq40137	Mac address not being learnt when "auth port-control auto" command is present
CSCvq55779	Five gig interface not showing in cli while configuring ip igmp snooping

Identifier	Description
CSCvq72713	Cat3k/Cat9k can't forwarding traffic follow the rule of EIGRP unequal cost load-balancing
CSCvq93773	C9600/9400/9500H/9300 etc crashes due to CMCC heartbeat failures
CSCvr04551	Multicast stream flickers on igmp join/leave
CSCvr07162	system crash on execute "fed TCAM utilization"
CSCvr46931	ports remain down/down object-manager (fed-ots-mo thread is stuck)
CSCvr71158	Commands returning invalid PRC error message

Troubleshooting

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

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

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

Related Documentation

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

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

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

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: 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 Marketplace.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

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.