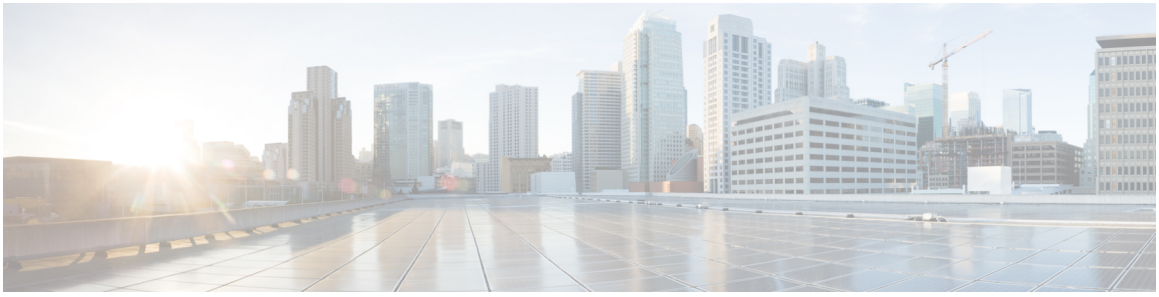
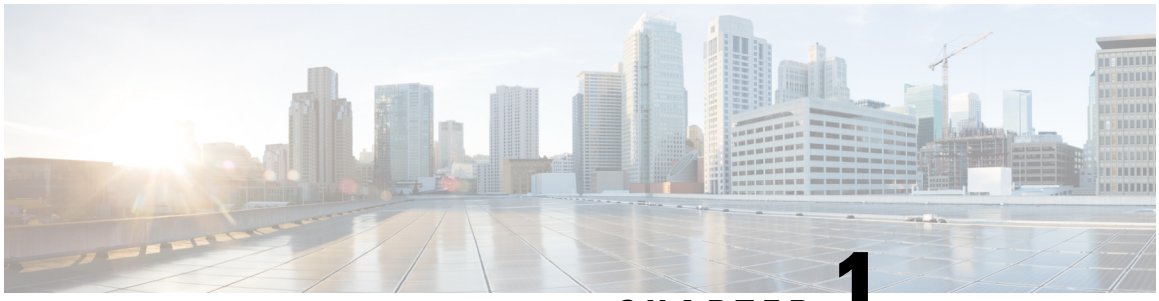
Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Dublin 17.12.x

First Published: 2023-07-28

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS



CHAPTER 1

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.

• Supported Hardware, on page 1

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
C9300-24H-A	Network Advantage	Stackable 24 10/100/1000 Mbps UPOE+ ports; PoE budget of 830 W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-24H-E	Network Essentials	
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	

Switch Model	Default License Level[1]	Description
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	
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	

Switch Model	Default License Level[1]	Description
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	
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	
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	

Switch Model	Default License Level[2]	Description
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	
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.

Table 3: Cisco Catalyst 9300LM Series Switches

Switch Model	Default License Level[3]	Description
C9300LM-48T-4Y-A	Network Advantage	Stackable 48 x 10/100/1000 M Ethernet ports; 4 x 25 GE SFP28 fixed uplink ports; 600 WAC power supply and fixed fans; supports StackWise-320.
C9300LM-48T-4Y-E	Network Essentials	

Switch Model	Default License Level[3]	Description
C9300LM-24U-4Y-A	Network Advantage	Stackable 24 x 10/100/1000 M UPOE ports; 4 x 25 GE SFP28 fixed uplink ports; PoE budget of 420 W with a single default 600 WAC power supply; supports StackWise-320.
C9300LM-24U-4Y-E	Network Essentials	
C9300LM-48U-4Y-A	Network Advantage	Stackable 48 x 10/100/1000 M UPOE ports; 4 x 25 GE SFP28 fixed uplink ports; PoE budget of 790 W with a single default 1000 WAC power supply; supports StackWise-320.
C9300LM-48U-4Y-E	Network Essentials	
C9300LM-48UX-4Y-A	Network Advantage	Stackable 40 x 10/100/1000 M and 8 Multigigabit Ethernet (100M/1000M/2.5GE/5GE/10GE) UPOE ports; 4 x 25 GE SFP28 fixed uplink ports; PoE budget of 790 W with a single default 1000 WAC power supply; supports StackWise-320.
C9300LM-48UX-4Y-E	Network Essentials	

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

Table 4: Cisco Catalyst 9300X Series Switches

Switch Model	Default License Level[4]	Description
C9300X-12Y-A	Network Advantage	Stackable 12 1/10/25 GE SFP28 downlink ports; 715 WAC power supply; supports StackPower+, StackWise-1T and C9300X-NM network modules.
C9300X-12Y-E	Network Essentials	
C9300X-24Y-A	Network Advantage	Stackable 24 1/10/25 GE SFP28 downlink ports; 715 WAC power supply; supports StackPower+, StackWise-1 and C9300X-NM network modules.
C9300X-24Y-E	Network Essentials	
C9300X-24HX-A	Network Advantage	Stackable 24 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE+ ports; PoE budget of 735W with 1100WAC power supply; supports StackPower+, StackWise-1T and C9300X-NM network modules.
C9300X-24HX-E	Network Essentials	
C9300X-48HX-A	Network Advantage	Stackable 48 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE+ports; PoE budget of 590W with 1100 WAC power supply; supports StackPower+, StackWise-1T and C9300X-NM network modules.
C9300X-48HX-E	Network Essentials	
C9300X-48TX-A	Network Advantage	Stackable 48 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) ports; 715WAC powersupply; supports StackPower+, StackWise-1T and C9300X-NM network modules.
C9300X-48TX-E	Network Essentials	

[4] 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.

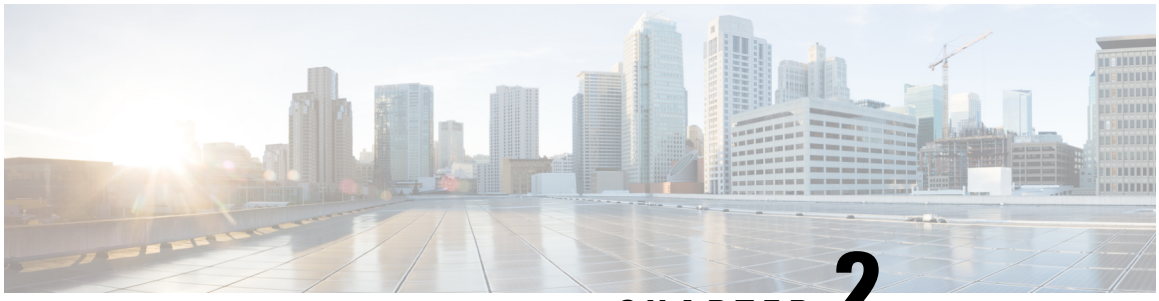
Network Module	Description
C3850-NM-4-1G [1]	Four 1 Gigabit Ethernet SFP module slots
C3850-NM-2-10G [1]	Two 10 Gigabit Ethernet SFP module slots
C3850-NM-4-10G [1]	Four 10 Gigabit Ethernet SFP module slots
C3850-NM-8-10G [1]	Eight 10 Gigabit Ethernet SFP module slots
C3850-NM-2-40G [1]	Two 40 Gigabit 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
C9300X-NM-2C[3]	Two 40 Gigabit Ethernet/100 Gigabit Ethernet QSFP+ module slots
C9300X-NM-4C [3]	Four 40 Gigabit Ethernet/100 Gigabit Ethernet slots with a QSFP+ connector ineach slot.
C9300X-NM-8M[3]	Eight Multigigabit Ethernet slots
C9300X-NM-8Y[3]	Eight 25 Gigabit Ethernet/10 Gigabit Ethernet/1 Gigabit Ethernet SFP+ 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.
3. These network modules are supported only on the C9300X SKUs of the Cisco Catalyst 9300 Series Switches.

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



CHAPTER 2

What's New in Cisco IOS XE Dublin 17.12.x

Hardware Features in Cisco IOS XE Dublin 17.12.1

Feature Name	Description
Cisco QSFP28 to SFP28 Adapter Module on Cisco Catalyst 9300X Series Switches	Supported transceiver module product number: • CVR-QSFP28-SFP25G Compatible switch models: • C9300X-12Y • C9300X-24Y • C9300X-48HX • C9300X-48TX • C9300X-24HX

Software Features in Cisco IOS XE Dublin 17.12.1

Feature Name	Description
BGP EVPN VXLAN • ARP inspection and DHCP Rogue Server Protection in VXLAN Environment (L2 VNIs) • BGP EVPN VRF Auto RD and Auto RT	The following BGP EVPN VXLAN features are introduced in this release: • ARP inspection and DHCP Rogue Server Protection in VXLAN Environment (L2 VNIs): BGP EVPN VXLAN fabric now supports ARP inspection and DHCP Rogue Server Protection. To configure these features, enable ARP inspection and DHCP Snooping on the VTEPs of the EVPN VXLAN fabric. • BGP EVPN VRF Auto RD and Auto RT: BGP EVPN Layer 3 overlay VRF configuration is simplified with the introduction of new CLIs to auto generate the route distinguisher (RD) and route target (RT) for a VRF. You can enable the auto generation of RD either at a global level, using the **vrf rd-auto** command or specifically for a VRF, using the **rd-auto** [**disable**] command in the VRF submode. To enable auto assignment of RT for a VRF, use the **vnid** *vni-id* command in the VRF submode. You can also choose to disable the auto RD and RT features by using the **no** form of the command.
DSCP marking for RADIUS packets for administrative sessions	Allows you to configure DSCP marking for RADIUS packets for administrative sessions such as SSH and Telnet.
EPC support of AppGigabitEthernet	Introduces support for configuring the AppGigabitEthernet port as an interface for Embedded Packet Capture (EPC).
Interface ID Option in DHCPv6 Relay Message	Introduces support for interface ID option in DHCPv6 Relay message. With this, the physical interface details of the client interface are included along with the VLAN number in the message.
IP DHCP Server Changes to Limit IP Assignment to Next Hop only	Allows you to assign DHCP IP address only to the neighbouring device in an interface using the **ip dhcp restrict next hop** command. When this command is enabled, the DHCP server in the interface uses the MAC addresses in the DHCP packet and compares it with the addresses in the Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) cache table. If the MAC addresses match, then the DHCP IP address is assigned to that device.

Feature Name	Description
Modified Trustpoints for Secure Unique Device Identity (SUDI) Certificates	

Feature Name	Description

	Starting from Cisco IOS XE Dublin 17.12.1, the following changes have been introduced for trustpoints.
	• Trustpoint names for existing SUDI certificates
	If your device supports Cisco Manufacturing CA III certificate and is not disabled, the trustpoint names are as follows.
	• For *Cisco Manufacturing CA III* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA3_SUDI
	• For *Cisco Manufacturing CA SHA2* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA2_SUDI
	If your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled using **no platform sudi cmca3** command, the trustpoint names are as follows.
	• For *Cisco Manufacturing CA SHA2* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA2_SUDI
	• For *Cisco Manufacturing CA* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA_SUDI
	• Hardware SUDI certificates
	• If your device supports *High Assurance SUDI CA* certificate, this certificate is loaded under CISCO_IDEVID_SUDI trustpoint.
	• If your device does not support *High Assurance SUDI CA* certificate, *ACT2 SUDI CA* certificate is loaded under CISCO_IDEVID_SUDI trustpoint.
	• **show wireless management trustpoint** command output
	If Cisco Catalyst 9300 Series Switch is used with a Cisco Embedded Wireless Controller for wireless deployments, the trustpoint name in the output of **show wireless management trustpoint** command is updated to the modified trustpoint name as mentioned previously.
	The following example shows a sample output of **show wireless management trustpoint** command. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the Trustpoint Name in the below output displays CISCO_IDEVID_CMCA2_SUDI.
	`Device# show wireless management trustpoint`
	`Trustpoint Name  : CISCO_IDEVID_CMCA3_SUDI`
	`Certificate Info : Available`
	`Certificate Type : MIC`
	`Certificate Hash : <SHA1 - hash>`
	`Private key Info : Available`
	`FIPS suitability : Not Applicable`
	• **show ip http server status** command output
	If you configure the trustpoint for the HTTP server as CISCO_IDEVID_SUDI, the output of **show ip http server status** command displays the operating trustpoint along with the configured trustpoint.
	The following example shows a sample output of **show ip http server status** command with

Feature Name	Description

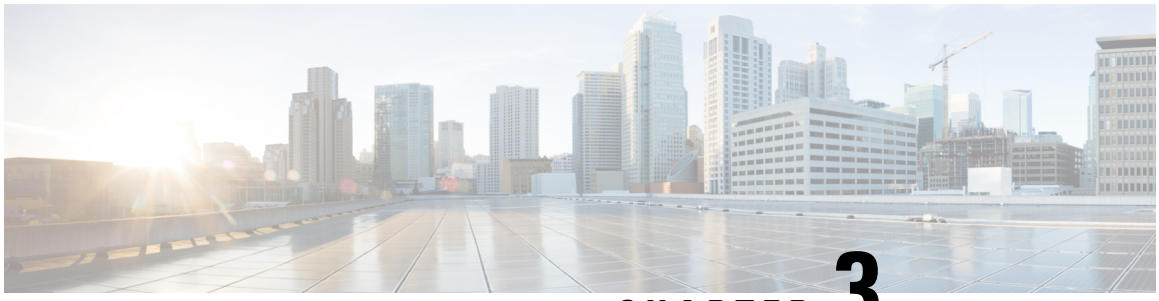
	both the configured and the operating trustpoint names. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the operating trustpoint in the below output displays CISCO_IDEVID_CMCA2_SUDI.
	`Device# show ip http server status`
	`…`
	`HTTP secure server trustpoint: CISCO_IDEVID_SUDI`
	`HTTP secure server operating trustpoint: CISCO_IDEVID_CMCA3_SUDI`

Programmability: • NETCONF-SSH Algorithms • YANG Data Models	The following programmability features are introduced in this release: • NETCONF-SSH Algorithms: The NETCONF-SSH server configuration file contains the list of all supported algorithms. From this release onwards, you can enable or disable these algorithms at runtime by using Cisco IOS commands or YANG models. • 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/17121.
request tech-support command	The **request tech-support** command was introduced. It generates an archive of tech support file and system report.
show idprom tan command	The **show idprom tan** command was introduced. It displays the top assembly part number and top assembly part revision number for the identification programmable read-only memory.

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

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.1

Behavior Change	Description
BDPU Guard and Root Guard Syslogs	The BDPU guard and root guard syslogs have been modified to include client bridge ID information.
system env fan-fail-action shut command	The expected behavior of the **system env fan-fail-action shut** command is fixed. When the command is enabled, the device automatically shuts down if more than one fan stops working or are removed.



CHAPTER 3

Important Notes

Important Notes

Unsupported Features

- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Converged Access for Branch Deployments
- MACsec switch-to-host connections in an overlay network.
- Performance Monitoring (PerfMon)
- Virtual Routing and Forwarding (VRF)-Aware web authentication
- Network Load Balancing (NLB)

Complete List of Supported Features

For the complete list of features supported on a platform, see the Cisco Feature Navigator.

Accessing Hidden Commands

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

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

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

- Category 1—Hidden commands in privileged or User EXEC mode. Begin by entering the **service internal** command to access these commands.
- Category 2—Hidden commands in one of the configuration modes (global, interface and so on). These commands do not require the **service internal** command.

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

- The commands have CLI help. 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.

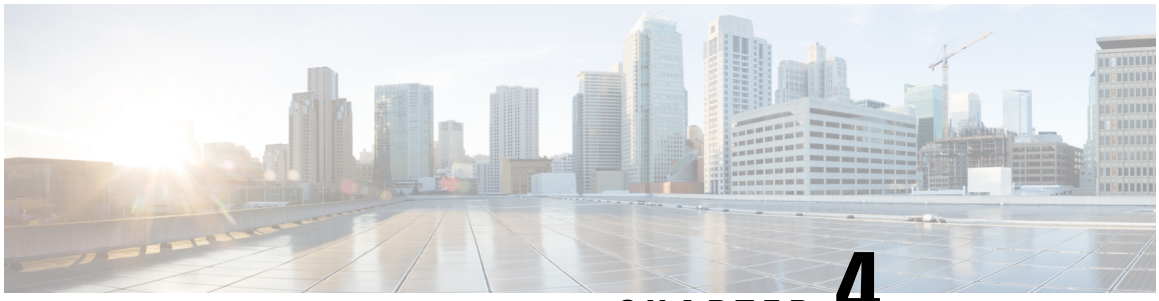
- The system generates a %PARSER-5-HIDDEN syslog message when a hidden command is used. For example:

```
*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.



CHAPTER 4

Compatibility Matrix and Web UI System Requirements

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
Dublin 17.12.1	3.2 3.1 + Patch 3 3.0 + Patch 6 2.7 + Patch 7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Dublin 17.11.1	3.2 3.1 + Patch 3 3.0 + Patch 6 2.7 + Patch 7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Dublin 17.10.1	3.2 3.1 + Patch 1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	C9300, C9300L, and C9300X: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Cupertino 17.9.4	3.2 3.1 + Patch 1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	C9300, C9300L, and C9300X: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Cupertino 17.9.3	3.2 3.1 + Patch 1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	C9300, C9300L, and C9300X: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Cupertino 17.9.2	3.2 3.1 + Patch 1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	C9300, C9300L, and C9300X: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Cupertino 17.9.1	3.2 3.1 + Patch 1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	C9300, C9300L, C9300LM, and C9300X: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Cupertino 17.8.1	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	C9300, C9300L, and C9300X: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.

Catalyst 9300	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	-	C9300, C9300L, and C9300X: 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	-	C9300, C9300L, and C9300X: 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	-	C9300, C9300L, and C9300X: 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	-	C9300, C9300L, and C9300X: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Bengaluru 17.6.3	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	C9300, C9300L, and C9300X: 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	-	C9300, C9300L, and C9300X: PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Bengaluru 17.6.1	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	C9300, C9300L, and C9300X: 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	-	C9300, C9300L, and C9300X: 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	-	C9300 and C9300L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Amsterdam 17.3.7	2.7	-	C9300 and C9300L: 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	-	C9300 and C9300L: 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	-	C9300 and C9300L: 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	-	C9300 and C9300L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Amsterdam 17.3.3	2.7	-	C9300 and C9300L: 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	-	C9300 and C9300L: 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	-	C9300 and C9300L: 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	-	C9300 and C9300L: 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	-	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.
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.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
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**.
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**.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
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**.
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**.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Fuji 16.9.3	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.2	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.1	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.8.1a	2.3 Patch 1 2.4	5.4 5.5	PI 3.3 + PI 3.3 latest maintenance release + PI 3.3 latest device pack See Cisco Prime Infrastructure 3.3→ **Downloads**.
Everest 16.6.4a	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.4	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.3	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
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[5]	512 MB[6]	256	1280 x 800 or higher	Small

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

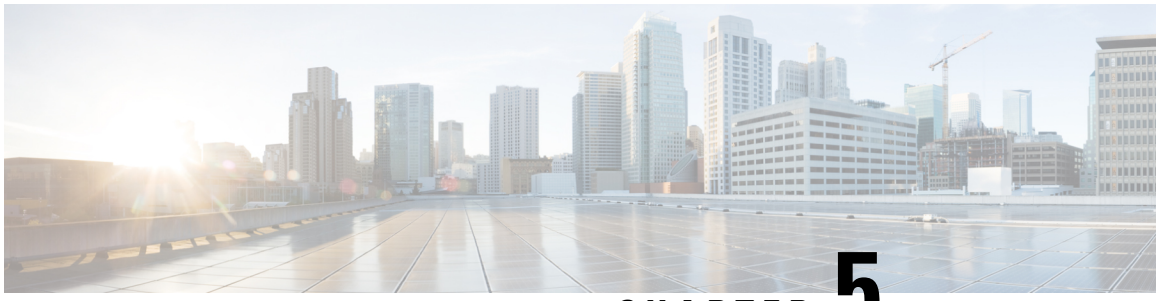
Software Requirements

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)



CHAPTER 5

Licensing and Scaling Guidelines

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.

Available Licensing Models and Configuration Information

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

  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 Essentials and Network-Advantage) are ordered and fulfilled only with a perpetual or permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a subscription or term license type.
- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- When ordering an add-on license with a base license, note the combinations that are permitted and those that are not permitted:

Table 5: Permitted Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No
Network Advantage	Yes[7]	Yes

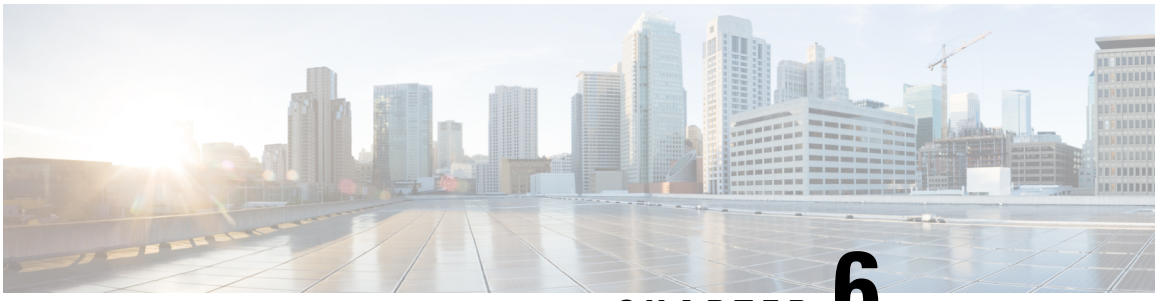
[7] You will be able to purchase this combination only at the time of the DNA license renewal and not when you purchase DNA-Essentials the first time.

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

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



CHAPTER 6

Limitations and Restrictions

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.
- Hardware Limitations—Optics:
  - SFP-10G-T-X supports 100Mbps/1G/10G speeds based on auto negotiation with the peer device. 10Mbps speed is not supported and you cannot force speed settings from the transceiver.
  - PHY Loopback test is not supported on SFP-10G-T-X.
- 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.
  - 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.

- 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).

  This limitation is removed from Cisco IOS XE Cupertino 17.9.1. If you configure a hostname and disable hostname privacy (**no license smart privacy hostname** global configuration command), hostname information is sent from the product instance and displayed on the applicable user interfaces (CSSM, CSLU, SSM On-Prem). For more information, see the command reference for this release.

- 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:

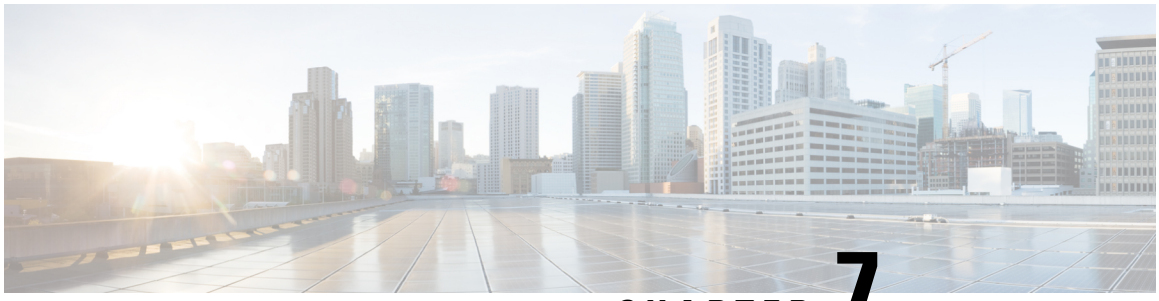
```
Device(config)# password encryption aes
Master key change notification called without new or old key
```

- Catatyst 9000 Series Switches support MACsec switch-to-switch connections. We do not recommend configuring MACsec switch-to-host connections in an overlay network. For assistance with an existing

switch-to-host MACsec implementation or a design review, contact your Cisco Sales Representative or Channel Partner.

- 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.

Limitations and Restrictions



CHAPTER 7

ROMMON Versions

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.

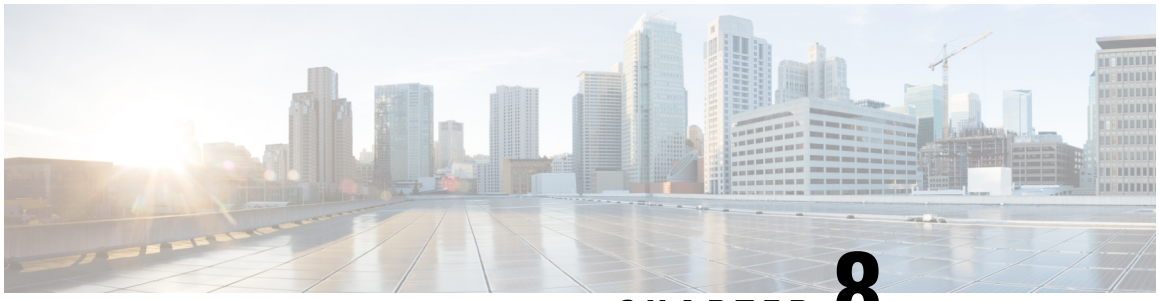
ROMMON upgrades may be required to resolve firmware defects, or to support new features, but there may not be new versions with every release.

Release	ROMMON Version (C9300 Models)	ROMMON Version (C9300L Models)	ROMMON Version (C9300X Models)	ROMMON Version (C9300LM Models)
Dublin 17.12.1	17.12.1r	17.12.1r	17.12.1r[FC1]	17.12.1r
Dublin 17.11.1	17.11.1r[FC1]	17.10.1r[FC1]	17.11.1r	17.10.1r

Release	ROMMON Version (C9300 Models)	ROMMON Version (C9300L Models)	ROMMON Version (C9300X Models)
Dublin 17.10.1	17.8.1r[FC2]	17.10.1r[FC1]	17.9.1r
Cupertino 17.9.4	17.9.2r	17.9.1r	17.9.1r
Cupertino 17.9.3	17.9.2r	17.9.1r	17.9.1r
Cupertino 17.9.2	17.8.1r[FC2]	17.8.1r[FC2]	17.5.1r
Cupertino 17.9.1	17.8.1r[FC2]	17.8.1r[FC2]	17.5.1r
Cupertino 17.8.1	17.8.1r[FC2]	17.8.1r[FC2]	17.5.1r

Release	ROMMON Version (C9300 Models)	ROMMON Version (C9300L Models)	ROMMON Version (C9300X Models)
Cupertino 17.7.1	17.6.1r[FC2]	17.6.1r[FC2]	17.5.1r
Bengaluru 17.6.6	17.6.1r[FC2]	17.8.1r[FC2]	17.5.1r
Bengaluru 17.6.5	17.6.1r[FC2]	17.8.1r[FC2]	17.5.1r
Bengaluru 17.6.4	17.6.1r[FC2]	17.8.1r[FC2]	17.5.1r
Bengaluru 17.6.3	17.6.1r[FC2]	17.8.1r[FC2]	17.5.1r
Bengaluru 17.6.2	17.6.1r[FC2]	17.8.1r[FC2]	17.5.1r
Bengaluru 17.6.1	17.6.1r[FC2]	17.8.1r[FC2]	17.5.1r
Bengaluru 17.5.1	17.5.2r	17.4.1r[FC2]	17.5.1r

Release	ROMMON Version (C9300 Models)	ROMMON Version (C9300L Models)
Bengaluru 17.4.1	17.4.1r	17.4.1r[FC2]
Amsterdam 17.3.7	17.3.2r	17.3.2r
Amsterdam 17.3.6	17.3.2r	17.3.2r
Amsterdam 17.3.5	17.3.2r	17.3.2r
Amsterdam 17.3.4	17.3.2r	17.3.2r
Amsterdam 17.3.3	17.3.2r	17.3.2r
Amsterdam 17.3.2a	17.3.2r	17.3.2r
Amsterdam 17.3.1	17.3.1r[FC2]	17.1.1r [FC1]
Amsterdam 17.2.1	17.2.1r[FC1]	17.1.1r[FC1]
Amsterdam 17.1.1	17.1.1r [FC1]	17.1.1r [FC1]



CHAPTER 8

Upgrading the Switch 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 Dublin 17.12.1	CAT9K_IOSXE	cat9k_iosxe.17.12.01.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.12.01.

Upgrading the ROMMON

To know the ROMMON or bootloader version that applies to every major and maintenance release, see ROMMON Versions, on page 35.

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 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.

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.

Summary of Software Installation Commands Supported starting from Cisco IOS XE Everest 16.6.2 and later releases	
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
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 Dublin 17.12.x
Cisco IOS XE Everest 16.6.2 and all later releases	Either **install** commands or **request platform software** commands[8].	

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

The sample output in this section displays upgrade from Cisco IOS XE Dublin 17.11.1 to Cisco IOS XE Dublin 17.12.1 using **install** commands only.

Procedure

Step 1 Clean-up

install remove inactive

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

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

```
Switch# install remove inactive

install_remove: START Wed Jul 24 10:02:31 PDT 2023
install_remove: Removing IMG
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 ...
[R0]: /flash/packages.conf File is in use, will not delete.
[R1]: /flash/packages.conf File is in use, will not delete.
[R0]: /flash/cat9k-cc_srdriver.17.11.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-cc_srdriver.17.11.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-espbase.17.11.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-espbase.17.11.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-guestshell.17.11.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-guestshell.17.11.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-lni.17.11.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-lni.17.11.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-rpbase.17.11.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-rpbase.17.11.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-sipbase.17.11.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-sipbase.17.11.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-sipspa.17.11.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-sipspa.17.11.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-srdriver.17.11.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-srdriver.17.11.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-webui.17.11.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-webui.17.11.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-wlc.17.11.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-wlc.17.11.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k_iosxe.17.11.01.SPA.conf File is in use, will not delete.
[R1]: /flash/cat9k_iosxe.17.11.01.SPA.conf File is in use, will not delete.
[R0]: /flash/cat9k-rpboot.17.11.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-rpboot.17.11.01.SPA.pkg File is in use, will not delete.

The following files will be deleted:
[R0]: /flash/cat9k_iosxe.17.11.01.SPA.bin
[R1]: /flash/cat9k_iosxe.17.11.01.SPA.bin
[R0]: /flash/cat9k-cc_srdriver.17.09.02.SPA.pkg
[R1]: /flash/cat9k-cc_srdriver.17.09.02.SPA.pkg
[R0]: /flash/cat9k-espbase.17.09.02.SPA.pkg
[R1]: /flash/cat9k-espbase.17.09.02.SPA.pkg
[R0]: /flash/cat9k-guestshell.17.09.02.SPA.pkg
[R1]: /flash/cat9k-guestshell.17.09.02.SPA.pkg
[R0]: /flash/cat9k-lni.17.09.02.SPA.pkg
```

```
[R1]: /flash/cat9k-lni.17.09.02.SPA.pkg
[R0]: /flash/cat9k-rpbase.17.09.02.SPA.pkg
[R1]: /flash/cat9k-rpbase.17.09.02.SPA.pkg
[R0]: /flash/cat9k-sipbase.17.09.02.SPA.pkg
[R1]: /flash/cat9k-sipbase.17.09.02.SPA.pkg
[R0]: /flash/cat9k-sipspa.17.09.02.SPA.pkg
[R1]: /flash/cat9k-sipspa.17.09.02.SPA.pkg
[R0]: /flash/cat9k-srdriver.17.09.02.SPA.pkg
[R1]: /flash/cat9k-srdriver.17.09.02.SPA.pkg
[R0]: /flash/cat9k-webui.17.09.02.SPA.pkg
[R1]: /flash/cat9k-webui.17.09.02.SPA.pkg
[R0]: /flash/cat9k-wlc.17.09.02.SPA.pkg
[R1]: /flash/cat9k-wlc.17.09.02.SPA.pkg
[R0]: /flash/cat9k_iosxe.17.09.02.SPA.conf
[R1]: /flash/cat9k_iosxe.17.09.02.SPA.conf
[R0]: /flash/cat9k-rpboot.17.09.02.SPA.pkg
[R1]: /flash/cat9k-rpboot.17.09.02.SPA.pkg

Do you want to remove the above files? [y/n]y

Deleting file /flash/cat9k_iosxe.17.11.01.SPA.bin ... done.
Deleting file /flash/cat9k-cc_srdriver.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-espbase.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-guestshell.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-lni.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-rpbase.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-sipbase.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-sipspa.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-srdriver.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-webui.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-wlc.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k_iosxe.17.09.02.SPA.conf ... done.
Deleting file /flash/cat9k-rpboot.17.09.02.SPA.pkg ... done.
Deleting /flash/.images/17.11.01.0.1444.1669767962 ... done.
SUCCESS: Files deleted.

--- Starting Post_Remove_Cleanup ---
Performing REMOVE_POSTCHECK on all members
Finished Post_Remove_Cleanup
SUCCESS: install_remove Wed Jul 24 10:02:36 PDT 2023
Switch#
<output truncated>
```

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.17.12.01.SPA.bin flash:

destination filename [cat9k_iosxe.17.12.01.SPA.bin]?
Accessing tftp://10.8.0.6/image/cat9k_iosxe.17.12.01.SPA.bin...
Loading /cat9k_iosxe.17.12.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]

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

b) **dir flash:**

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

```
Switch# dir flash:*.bin

Directory of flash:/*.bin

Directory of flash:/

434184 -rw- 601216545    Jul 24 2023 10:18:11 -07:00 cat9k_iosxe.17.12.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

Step 3 Set boot variable

a) **no boot system**

Use this command to reset the boot variable. This command removes the startup system image specification. Otherwise, the switch may boot a previously configured boot image.

```
Switch(config)# no boot system
```

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

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

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

c) **no boot manual**

Use this command to configure the switch to auto-boot.

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

d) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

e) **show boot**

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

```
Switch# show boot
Current Boot Variables:
BOOT variable = flash:packages.conf;

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

Step 4 Install image to flash

install add file activate commit

Use this command to install the image.

We recommend that you point to the source image on your TFTP server or the flash drive of the *active* switch, if you have copied the image to flash memory. If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For

example, if the image is on the flash drive of member switch 3 (flash-3): `Switch# **install add file flash-3:cat9k_iosxe.17.12.01.SPA.bin activate commit**`.

The following sample output displays installation of the Cisco IOS XE Dublin 17.12.1 software image in the flash memory:

```
Switch# install add file flash:cat9k_iosxe.17.12.01.SPA.bin activate commit

install_add_activate_commit: START Wed Jul 24 10:15:02 PDT 2023
install_add: START Wed Jul 24 10:15:02 PDT 2023
install_add: Adding IMG
--- Starting initial file syncing ---
Copying flash:cat9k_iosxe.17.12.01.SPA.bin from Switch 1 to Switch 1 2
Info: Finished copying to the selected Switch
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
 [1] Finished Add package(s) on Switch 1
 [2] Finished Add package(s) on Switch 2
Checking status of Add on [1 2]
Add: Passed on [1 2]
Finished Add

Image added. Version: 17.12.01.0

    Warning: ISSU compatibility check failed for 17.12.01.0
install_activate: START Wed Jul 24 10:17:34 PDT 2023
install_activate: Activating IMG
Following packages shall be activated:
/flash/cat9k-cc_srdriver.17.12.01.SPA.pkg
/flash/cat9k-espbase.17.12.01.SPA.pkg
/flash/cat9k-guestshell.17.12.01.SPA.pkg
/flash/cat9k-lni.17.12.01.SPA.pkg
/flash/cat9k-rpbase.17.12.01.SPA.pkg
/flash/cat9k-sipbase.17.12.01.SPA.pkg
/flash/cat9k-sipspa.17.12.01.SPA.pkg
/flash/cat9k-srdriver.17.12.01.SPA.pkg
/flash/cat9k-webui.17.12.01.SPA.pkg
/flash/cat9k-wlc.17.12.01.SPA.pkg
/flash/cat9k-rpboot.17.12.01.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
 [2] Activate package(s) on Switch 2
 [2] Finished Activate on Switch 2
 [1] Finished Activate on Switch 1
Checking status of Activate on [1 2]
Activate: Passed on [1 2]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
 [1] Commit package(s) on Switch 1
 [2] Commit package(s) on Switch 2
 [1] Finished Commit on Switch 1
 [2] Finished Commit on Switch 2
Checking status of Commit on [1 2]
Commit: Passed on [1 2]
Finished Commit operation
```

```
*Jul 24 10:22:00.934: %IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): Starting boot preupgrade
*Jul 24 10:22:00.937: %IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Wed Jul 24 10:22:00 PDT
 2023 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING
*Jul 24 10:22:50.808: %IOSXEBOOT-4-flashcp: (rp/0): polaris_adelphi_rommon_sb.bin
*Jul 24 10:22:56.093: %IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): boot loader upgrade successful



       SUCCESS: install_add_activate_commit Wed Jul 24 10:22:59 PDT 2023
stack-nyqcr3#
Chassis 1 reloading, reason - Reload command
Jul 24 10:23:05.604: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
Jul 24 10:23:07.295: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes
 exit with reload switch code



Initializing Hardware......

System Bootstrap, Version 17.12.1r[FC1], RELEASE SOFTWARE (P)
Compiled Wed 02/07/2023 14:36:07.63 by rel

Current ROMMON image : Primary
Last reset cause     : SoftwareReload
C9300-48UXM platform with 8388608 Kbytes of main memory

Preparing to autoboot. [Press Ctrl-C to interrupt]  0
boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf
################################################################################################################################
################################################################################################################################


Waiting for 120 seconds for other switches to boot

Switch number is 1
All switches in the stack have been discovered. Accelerating discovery
<output truncated>
```

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

Step 5 Verify installation

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

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

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

```
Switch# dir flash:*.pkg

Directory of flash:/
75140 -rw- 2012104     Mar 9 2023 09:52:41 -07:00 cat9k-cc_srdriver.17.11.01.SPA.pkg
475141 -rw- 70333380   Mar 9 2023 09:52:44 -07:00 cat9k-espbase.17.11.01.SPA.pkg
475142 -rw- 13256      Mar 9 2023 09:52:44 -07:00 cat9k-guestshell.17.11.01.SPA.pkg
475143 -rw- 349635524  Mar 9 2023 09:52:54 -07:00 cat9k-rpbase.17.11.01.SPA.pkg
475149 -rw- 24248187   Mar 9 2023 09:53:02 -07:00 cat9k-rpboot.17.11.01.SPA.pkg
475144 -rw- 25285572   Mar 9 2023 09:52:55 -07:00 cat9k-sipbase.17.11.01.SPA.pkg
475145 -rw- 20947908   Mar 9 2023 09:52:55 -07:00 cat9k-sipspa.17.11.01.SPA.pkg
475146 -rw- 2962372    Mar 9 2023 09:52:56 -07:00 cat9k-srdriver.17.11.01.SPA.pkg
475147 -rw- 13284288   Mar 9 2023 09:52:56 -07:00 cat9k-webui.17.11.01.SPA.pkg
```

```
475148 -rw- 13248      Mar 9 2023 09:52:56 -07:00 cat9k-wlc.17.11.01.SPA.pkg

491524 -rw- 25711568   Jul 24 2023 11:49:33 -07:00 cat9k-cc_srdriver.17.12.01.SPA.pkg
491525 -rw- 78484428   Jul 24 2023 11:49:35 -07:00 cat9k-espbase.17.12.01.SPA.pkg
491526 -rw- 1598412    Jul 24 2023 11:49:35 -07:00 cat9k-guestshell.17.12.01.SPA.pkg
491527 -rw- 404153288  Jul 24 2023 11:49:47 -07:00 cat9k-rpbase.17.12.01.SPA.pkg
491533 -rw- 31657374   Jul 24 2023 11:50:09 -07:00 cat9k-rpboot.17.12.01.SPA.pkg
491528 -rw- 27681740   Jul 24 2023 11:49:48 -07:00 cat9k-sipbase.17.12.01.SPA.pkg
491529 -rw- 52224968   Jul 24 2023 11:49:49 -07:00 cat9k-sipspa.17.12.01.SPA.pkg
491530 -rw- 31130572   Jul 24 2023 11:49:50 -07:00 cat9k-srdriver.17.12.01.SPA.pkg
491531 -rw- 14783432   Jul 24 2023 11:49:51 -07:00 cat9k-webui.17.12.01.SPA.pkg
491532 -rw- 9160       Jul 24 2023 11:49:51 -07:00 cat9k-wlc.17.12.01.SPA.pkg


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

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

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

- `packages.conf`—the file that has been re-written with the newly installed .pkg files
- `cat9k_iosxe.17.12.01.SPA.conf`— a backup copy of the newly installed packages.conf file

```
Switch# dir flash:*.conf

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

434197 -rw- 7406 Jul 24 2023 10:59:16 -07:00 packages.conf
516098 -rw- 7406 Jul 24 2023 10:58:08 -07:00 cat9k_iosxe.17.12.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

Step 6 **show version**

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

The following sample output of the **show version** command displays the Cisco IOS XE Dublin 17.12.1 image on the device:

```
Switch# show version

Cisco IOS XE Software, Version 17.12.01
Cisco IOS Software [Dublin], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.12.1,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2023 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 ...	Use these commands...	To downgrade to...
Cisco IOS XE Dublin 17.12.x	Either **install** commands or **request platform software** command[9].	Cisco IOS XE Dublin 17.11.x or earlier releases.

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

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

The sample output in this section shows downgrade from Cisco IOS XE Dublin 17.12.1 to Cisco IOS XE Dublin 17.11.1, using **install** commands.

Microcode Downgrade Prerequisite:

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 Cisco IOS XE Fuji 16.9.1 through Cisco IOS XE Fuji 16.9.2	**install** commands	Microcode will roll back automatically as part of the software installation. No further action is required.
		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.

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 Mon Jul 24 10:34:24 PDT 2023
install_remove: Removing IMG
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 ...
[R0]: /flash/packages.conf File is in use, will not delete.
[R1]: /flash/packages.conf File is in use, will not delete.
[R0]: /flash/cat9k-cc_srdriver.17.12.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-cc_srdriver.17.12.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-espbase.17.12.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-espbase.17.12.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-guestshell.17.12.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-guestshell.17.12.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-lni.17.12.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-lni.17.12.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-rpbase.17.12.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-rpbase.17.12.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-sipbase.17.12.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-sipbase.17.12.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-sipspa.17.12.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-sipspa.17.12.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-srdriver.17.12.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-srdriver.17.12.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-webui.17.12.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-webui.17.12.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-wlc.17.12.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-wlc.17.12.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k_iosxe.17.12.01.SPA.conf File is in use, will not delete.
[R1]: /flash/cat9k_iosxe.17.12.01.SPA.conf File is in use, will not delete.
[R0]: /flash/cat9k-rpboot.17.12.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-rpboot.17.12.01.SPA.pkg File is in use, will not delete.

The following files will be deleted:
[R0]: /flash/cat9k_iosxe.17.12.01.SPA.bin
[R1]: /flash/cat9k_iosxe.17.12.01.SPA.bin
[R0]: /flash/cat9k-cc_srdriver.17.09.02.SPA.pkg
[R1]: /flash/cat9k-cc_srdriver.17.09.02.SPA.pkg
[R0]: /flash/cat9k-espbase.17.09.02.SPA.pkg
[R1]: /flash/cat9k-espbase.17.09.02.SPA.pkg
[R0]: /flash/cat9k-guestshell.17.09.02.SPA.pkg
[R1]: /flash/cat9k-guestshell.17.09.02.SPA.pkg
[R0]: /flash/cat9k-lni.17.09.02.SPA.pkg
[R1]: /flash/cat9k-lni.17.09.02.SPA.pkg
[R0]: /flash/cat9k-rpbase.17.09.02.SPA.pkg
[R1]: /flash/cat9k-rpbase.17.09.02.SPA.pkg
[R0]: /flash/cat9k-sipbase.17.09.02.SPA.pkg
[R1]: /flash/cat9k-sipbase.17.09.02.SPA.pkg
[R0]: /flash/cat9k-sipspa.17.09.02.SPA.pkg
[R1]: /flash/cat9k-sipspa.17.09.02.SPA.pkg
[R0]: /flash/cat9k-srdriver.17.09.02.SPA.pkg
[R1]: /flash/cat9k-srdriver.17.09.02.SPA.pkg
[R0]: /flash/cat9k-webui.17.09.02.SPA.pkg
[R1]: /flash/cat9k-webui.17.09.02.SPA.pkg
[R0]: /flash/cat9k-wlc.17.09.02.SPA.pkg
[R1]: /flash/cat9k-wlc.17.09.02.SPA.pkg
[R0]: /flash/cat9k_iosxe.17.09.02.SPA.conf
```

```
[R1]: /flash/cat9k_iosxe.17.09.02.SPA.conf
[R0]: /flash/cat9k-rpboot.17.09.02.SPA.pkg
[R1]: /flash/cat9k-rpboot.17.09.02.SPA.pkg

Do you want to remove the above files? [y/n]y

Deleting file /flash/cat9k_iosxe.17.12.01.SPA.bin ... done.
Deleting file /flash/cat9k-cc_srdriver.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-espbase.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-guestshell.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-lni.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-rpbase.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-sipbase.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-sipspa.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-srdriver.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-webui.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-wlc.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k_iosxe.17.09.02.SPA.conf ... done.
Deleting file /flash/cat9k-rpboot.17.09.02.SPA.pkg ... done.
Deleting /flash/.images/17.12.01.0.172764.1674613814 ... done.
SUCCESS: Files deleted.

--- Starting Post_Remove_Cleanup ---
Performing REMOVE_POSTCHECK on all members
Finished Post_Remove_Cleanup
SUCCESS: install_remove Mon Jul 24 10:34:32 PDT 2023
```

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.17.11.01.SPA.bin flash:
Destination filename [cat9k_iosxe.17.11.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.17.11.01.SPA.bin...
Loading /cat9k_iosxe.17.11.01.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 24 2023 13:35:16 -07:00 cat9k_iosxe.17.11.01.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.

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

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show boot**

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

```
Switch# show boot

Current Boot Variables:
BOOT variable = flash:packages.conf;

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

Step 4 Downgrade software image

install add file activate commit

Use this command to install the image.

We recommend that you point to the source image on your TFTP server or the flash drive of the *active* switch, if you have copied the image to flash memory. If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For example, if the image is on the flash drive of member switch 3 (flash-3): `Switch# install add file flash-3:cat9k_iosxe.17.11.01.SPA.bin activate commit`.

The following example displays the installation of the Cisco IOS XE Dublin 17.11.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.17.11.01.SPA.bin activate commit

install_add_activate_commit: START Mon Jul 24 10:55:53 PDT 2023
install_add: START Mon Jul 24 10:55:53 PDT 2023
install_add: Adding IMG
 [2] Switch 2 Warning!!! Image is being downgraded from 17.12.01.0.1186 to 17.11.01.0.1444.
--- Starting initial file syncing ---
Copying flash:cat9k_iosxe.17.11.01.SPA.bin from Switch 1 to Switch 1 2
Info: Finished copying to the selected Switch
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
Checking status of Add on [1 2]
Add: Passed on [1 2]
Image added. Version: 17.11.01.0.1444

Finished Add

install_activate: START Mon Jul 24 10:57:32 PDT 2023
install_activate: Activating IMG
```

```
Following packages shall be activated:
/flash/cat9k-cc_srdriver.17.11.01.SPA.pkg
/flash/cat9k-espbase.17.11.01.SPA.pkg
/flash/cat9k-guestshell.17.11.01.SPA.pkg
/flash/cat9k-lni.17.11.01.SPA.pkg
/flash/cat9k-rpbase.17.11.01.SPA.pkg
/flash/cat9k-sipbase.17.11.01.SPA.pkg
/flash/cat9k-sipspa.17.11.01.SPA.pkg
/flash/cat9k-srdriver.17.11.01.SPA.pkg
/flash/cat9k-webui.17.11.01.SPA.pkg
/flash/cat9k-wlc.17.11.01.SPA.pkg
/flash/cat9k-rpboot.17.11.01.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
 [2] Activate package(s) on Switch 2
 [2] Finished Activate on Switch 2
 [1] Finished Activate on Switch 1
Checking status of Activate on [1 2]
Activate: Passed on [1 2]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
 [1] Commit package(s) on Switch 1
 [2] Commit package(s) on Switch 2
 [2] Finished Commit on Switch 2
 [1] Finished Commit on Switch 1
Checking status of Commit on [1 2]
Commit: Passed on [1 2]
Finished Commit operation

SUCCESS: install_add_activate_commit Mon Jul 24 11:00:19 PDT 2023
stack-nyqcr3#
Chassis 1 reloading, reason - Reload command
Jul 24 11:00:25.253: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
Jul 24 11:00:26.878: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes
 exit with reload switch code



Initializing Hardware......

System Bootstrap, Version 17.12.1r[FC1], RELEASE SOFTWARE (P)
Compiled Wed 02/08/2023 14:36:07.63 by rel

Current ROMMON image : Primary
Last reset cause     : SoftwareReload
C9300-48UXM platform with 8388608 Kbytes of main memory

Preparing to autoboot. [Press Ctrl-C to interrupt]  0
boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf
#
################################################################################################################################
################################################################################################################################
################################################################################################################################


Waiting for 120 seconds for other switches to boot
```

```
Switch number is 1
All switches in the stack have been discovered. Accelerating discovery
```

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 Dublin 17.11.1 image on the device:

```
Switch# show version

Cisco IOS XE Software, Version 17.11.01
Cisco IOS Software [Dublin], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.11.1,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2023 by Cisco Systems, Inc.
<output truncated>
```

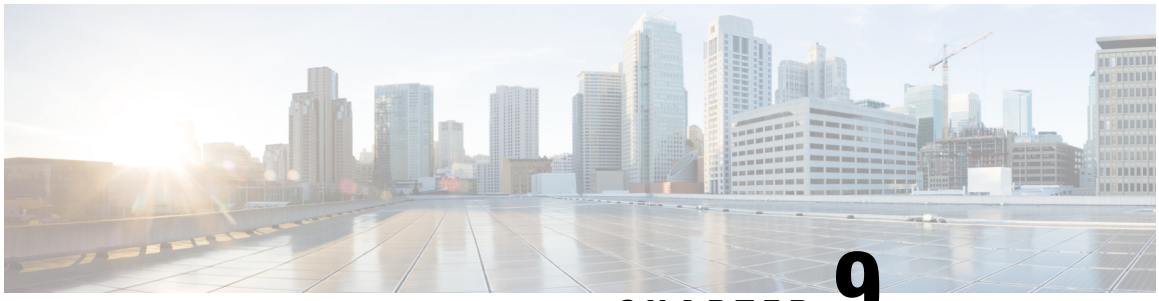
Field-Programmable Gate Array Version Upgrade

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

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

Note

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



CHAPTER 9

Caveats

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.

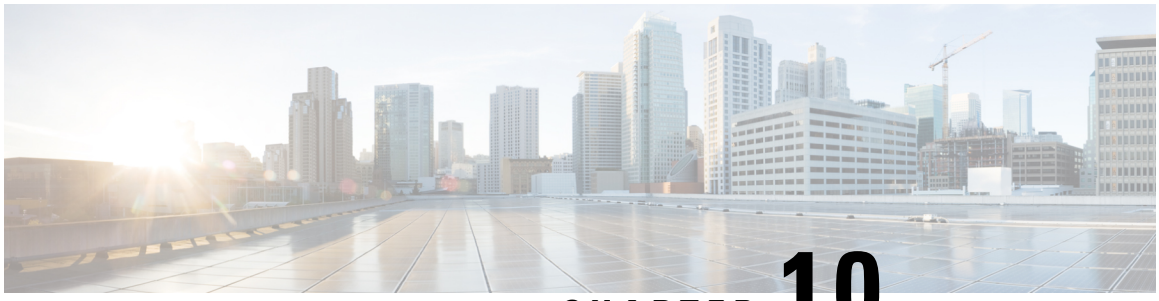
To view the details of a caveat, click on the identifier.

Open Caveats in Cisco IOS XE Dublin 17.12.x

Identifier	Headline
CSCwf62551	(C9300X) interop:Ports are not coming up between 9300X-Uplink and 9500X with "100G QSFP 100G CU3M"
CSCwh35728	Need switch to host macsec support in Sda overlay network

Resolved Caveats in Cisco IOS XE Dublin 17.12.1

Identifier	Headline
CSCwd99665	(C9300L) C9300L-48UXG-4X: TMPFS leak due to excessive logging to debug_logging_file



CHAPTER 10

Additional Information

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: http://www.cisco.com/go/mibs

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.

- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

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.