Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Amsterdam 17.3.x

First Published: 2020-08-10

Last Modified: 2023-10-30

Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Amsterdam 17.3.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 17.3.8a

There are no new features in this release. This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

Whats New in Cisco IOS XE Amsterdam 17.3.8

Hardware Features in Cisco IOS XE Amsterdam 17.3.8

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.8

There are no new software features in this release.

Whats New in Cisco IOS XE Amsterdam 17.3.7

Hardware Features in Cisco IOS XE Amsterdam 17.3.7

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.7

There are no new software features in this release.

Whats New in Cisco IOS XE Amsterdam 17.3.6

Hardware Features in Cisco IOS XE Amsterdam 17.3.6

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.6

There are no new software features in this release.

Whats New in Cisco IOS XE Amsterdam 17.3.5

Hardware Features in Cisco IOS XE Amsterdam 17.3.5

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.5

There are no new software features in this release.

Whats New in Cisco IOS XE Amsterdam 17.3.4

Hardware Features in Cisco IOS XE Amsterdam 17.3.4

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.4

There are no new software features in this release.

Whats New in Cisco IOS XE Amsterdam 17.3.3

Hardware Features in Cisco IOS XE Amsterdam 17.3.3

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.3

Feature Name	Description, Documentation Link, and License Level Information
Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy	SSM On-Prem is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM. Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. The product instance can be configured to *push* the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to *pull* the required information from a product instance at a configurable frequency. After usage information is available in SSM On-Prem, you must synchronize the same with CSSM, to ensure that the product instance count, license count and license usage information is the same on both, CSSM and SSM On□Prem. Offline and online options are available for synchronization between CSSM and SSM On□Prem. Minimum Required SSM On-Prem Version: Version 8, Release 202102. Minimum Required Cisco IOS XE Version: Cisco IOS XE Amsterdam 17.3.3. See System Mangement → Smart Licening Using Policy and System Management Commands. (A license level does not apply)
ThousandEyes Enterprise Agent	A new version of the ThousandEyes Enterprise Agent is introduced. This is an embedded Docker-based application that runs on Cisco devices using the application-hosting capability.The Enterprise Agent is available on both the SSD and bootflash. See Programmability Configuration Guide → Application Hosting. (Network Advantage)
MLDP-Based MVPN	The MLDP-based MVPN feature provides extensions to Label Distribution Protocol (LDP) for the setup of point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) label switched paths (LSPs) for transport in the Multicast Virtual Private Network (MVPN) core network. See IP Multicast Routing Configuration Guide → MLDP-Based MVPN. (Network Advantage)

Whats New in Cisco IOS XE Amsterdam 17.3.2a

Hardware Features in Cisco IOS XE Amsterdam 17.3.2a

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.2a

Feature Name	Description, Documentation Link, and License Level Information
Smart Licensing Using Policy	An enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use. With this licensing model, you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date. Multiple options are available for license usage reporting – this depends on the topology you implement. You can use the Cisco Smart Licensing Utility (CSLU) Windows application, or report usage information directly to CSSM. A provision for offline reporting for air-gapped networks, where you download usage information and upload to CSSM, is also available. Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to this release. By default, your Smart Account and Virtual Account in CSSM is enabled for Smart Licensing Using Policy. For conceptual, configuration, migration, and troubleshooting information for Smart Licensing Using Policy, see the documentation links below. See System Mangement → Smart Licening Using Policy and System Management Commands. (A license level does not apply)
Cisco DNA Center Support for Smart Licensing Using Policy	Cisco DNA Center supports Smart Licensing Using Policy functionality starting with Cisco DNA Center Release 2.2.2. The corresponding minimum required Cisco IOS XE Release on the Cisco Catalyst 9300 Series Switches (all models) is Cisco IOS XE Amsterdam 17.3.2a. Implement the “Connected to CSSM Through a Controller” topology to have Cisco DNA Center manage a product instance. When you do, the product instance records license usage, but it is the Cisco DNA Center that initiates communication with the product instance to retrieve and report usage to Cisco Smart Software Manager (CSSM), and returns the acknowledgement (RUM ACK). In order to meet reporting requirements, Cisco DNA Center provides ad hoc or on-demand reporting, as well as scheduled reporting options. See System Mangement → Smart Licening Using Policy. (A license level does not apply)
Extended Fast Software Upgrade	Extended Fast Software Upgrade reduces the traffic downtime to less than 30 seconds during software reload operations. See System Management → Extended Fast Software Upgrade. (Network Advantage)

Whats New in Cisco IOS XE Amsterdam 17.3.1

Hardware Features in Cisco IOS XE Amsterdam 17.3.1

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.1

Feature Name	Description, Documentation Link, and License Level Information
Active Directory Integration for Umbrella Connector	Introduces support for Active Directory Connector, which retrieves and uploads user and group information mapping from the on-premise active directory to the Umbrella Resolver, at regular intervals. Based on the pre-uploaded record of all users and groups in the Umbrella Resolver, the Umbrella Cloud applies the appropriate policy on the DNS packets it receives. See Security → Configuring Cisco Umbrella Integration. (Network Advantage)
BGP EVPN VXLAN • Broadcast, Unknown Unicast, and Multicast (BUM) Traffic Rate Limiting • Enhanced rendezvous point (RP) Functionality for Layer 3 TRM for IPv4 and IPv6 traffic • Interworking of Layer 3 TRM with MVPN Networks for IPv4 Traffic • Layer 3 Tenant Routed Multicast (TRM) for IPv6 Traffic	The following BGP EVPN VXLAN features are introduced in this release: • BUM Traffic Rate Limiting: Allows you to use a policer and set the flood rate limit of the BUM traffic in the network to a predefined value. • Enhanced RP Functionality for Layer 3 TRM for IPv4 and IPv6 traffic: Allows you to configure an RP for TRM with PIM-Sparse Mode (PIM-SM) on a single or multiple VTEPs inside the BGP EVPN VXLAN fabric or on a device outside the fabric. • Interworking of Layer 3 TRM with MVPN Networks for IPv4 Traffic: Allows you to forward IPv4 Layer 3 multicast traffic between sources and receivers of an EVPN VXLAN network and an MVPN network. • Layer 3 Tenant Routed Multicast for IPv6 Traffic: Introduces support to configure Layer 3 TRM for IPv6 traffic with PIM-Source Specific Mode (PIM-SSM) and with PIM-SM. See BGP EVPN VXLAN. (Network Advantage)
Enhanced SGACL Logging	Introduces support for Security Group Access Control List (SGACL) logging using NetFlow hardware, which allows much higher logging rates. See Cisco TrustSec → Configuring Security Group ACL Policies. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Link Aggregation Control Protocol (LACP) 1:1 Redundancy and Dampening	Introduces support for: • LACP 1:1 Redundancy: Supports an EtherChannel configuration with one active link and fast switchover to a hot standby link. • LACP 1:1 Hot Standby Dampening: Configures a timer that delays switchover back to the higher priority port after it becomes active. See Layer 2 → Configuring EtherChannels. (Network Essentials and Network Advantage)
MPLS QoS - WRED	Introduces support for weighted random early detection (WRED) in MPLS Quality of Service (QoS). This feature configures WRED to use the MPLS experimental bits (EXP) to calculate the drop probability of a packet. See Multiprotocol Label Switching → Configuring MPLS QoS. (Network Advantage)
MPLS VPN InterAS Option AB	Enables different autonomous systems to interconnect by using a single Multiprotocol Border Gateway Protocol (MP-BGP) session, which is enabled globally on the router. When different autonomous systems are interconnected in an MPLS VPN InterAS Option AB configuration, the entire network configuration is scaled and simplified, and maintains IP quality of service (QoS) functions between Autonomous System Boundary Router (ASBR) peers. See Multiprotocol Label Switching → Configuring MPLS VPN InterAS Options. (Network Advantage)
Private VLAN (PVLAN) on Trunk Ports and Portchannels	Enables configuration of private VLANs on isolated trunk ports, promiscuous trunk ports, and on port channels. See VLAN → Configuring Private VLANs. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Programmability • gNMI Configuration Persistence • gNOI Certificate Management • gNOI Bootstrapping with Certificate Service • YANG Data Models	The following programmability features are introduced in this release: • gNMI (gRPC Network Management Interface) Configuration Persistence: Ensures that all successful changes made through the gNMI SET RPC persist after a device restart. • gNOI Certificate Management: The gRPC Network Operations Interface (gNOI) Certificate Management service provides RPCs to install, rotate, get certificate, revoke certificate, and generate certificate signing request (CSR). • gNOI Bootstrapping with Certificate Service: After installing gNOI certificates, bootstrapping is used to configure or operate a target. gNMI bootstrapping is enabled by using the **gnxi-secure-int** command and disabled by using the **secure-allow-self-signed-trustpoint** command. • 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/1731. 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. (Network Essentials and Network Advantage)
Switch Integrated Security Features (SISF) - Throttling of ARP Packets	Starting with this release, ARP packets are throttled to mitigate high CPU utilization scenarios. In a five second window, a maximum of 50 ARP broadcast packets per binding entry are processed by SISF. When the limit is reached, incoming ARP packets are dropped. Note that the limit of 50 in five seconds is for each binding entry, that is, for each source IP.
VPLS: Routed Pseudowire IRB for IPv6 Unicast	Introduces IPv6 support for Virtual Private LAN Service (VPLS) Routed Pseudowire Integrated Routing and Bridging (IRB). VPLS Routed Pseudowire enables a switch interface to route traffic instead of using a router. See Multiprotocol Label Switching → Configuring VPLS: Routed Pseudowire IRB for IPv6 Unicast. (Network Advantage)
Forwarding Scale Enhancements	The forwarding scale numbers for the following features have changed: • Layer 2 Unicast MAC Addresses: 49152 • Layer 3 Multicast: 32768 • QoS Access Control Entries: 6144 • Policy Based Routing ACEs / NAT ACEs: 14336 Supported switch models—C9300-24UB, C9300-24UXB, C9300-48UB (Network Essentials and Network Advantage)

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

Serviceability	
monitor capture match	The command was modified. The following keywords were introduced: • **packet-length**: Specifies packet length filter for packet capture • **access-list**: Specifies access-list filter for packet capture
show bootflash:	The command was modified. The following keywords were introduced: • **namesort**: Sorts the output based on file name • **sizesort**: Sorts the output based on file size • **timesort**: Sorts the output based on the timestamp of the file
show logging process ios module	The command was introduced. It displays the logs of the specified IOS module.
show platform hardware fed active fwd-asic counters tla	• The command output was enhanced to display the TLA counters information. • The **change** keyword was deprecated.
show switch stack-ports	The command was modified. The **detail** keyword was introduced. It displays the stack interface link status and errors.
show mpls ldp	The command was introduced. It provides the following options: • **show mpls ldp discovery**: Displays the status of the LDP discovery process • **show mpls ldp neighbor**: Displays the status of LDP sessions. • **show mpls ldp bindings**: Displays the contents of the Label Information Base (LIB).
show tech-support	The command was modified. The following keywords were introduced: • **show tech-support confidential**: The **confidential** keyword was introduced, to mask sensitive information in the output of **show tech-support** command. • **show tech-support monitor**: The **monitor** keyword was introduced. It displays Switched Port Analyzer (SPAN) monitor-related information. • **show tech-support pvlan**: The **pvlan** keyword was introduced. It displays Private VLAN-related information.
System Report Files - Hostname	In a complex network it is difficult to track the origin of a system-report file. In order to make the reports easily and uniquely identifiable, the hostname is now prepended to the system-report file name.

Important Notes

• Unsupported Features, on page 9

- Complete List of Supported Features, on page 9
- Accessing Hidden Commands, on page 9
- Default Behaviour, on page 10

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://cfnng.cisco.com.

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.

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
C9300-24H-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	
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	

Switch Model	Default License Level[1]	Description
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	
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	

Switch Model	Default License Level[1]	Description
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	

Switch Model	Default License Level[2]	Description
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	
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	

Switch Model	Default License Level[2]	Description
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.

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

Network Module	Description
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 17.3.8a	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 17.3.8	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 17.3.7	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**.
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**.

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

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

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

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
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[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 17.3.8a	17.3.8r	17.8.1r[FC2]	-	-
Amsterdam 17.3.8	17.3.8r	17.8.1r[FC2]	-	-
Amsterdam 17.3.7	17.3.2r	17.8.1r[FC2]	-	-
Amsterdam 17.3.6	17.3.2r	17.8.1r[FC2]	-	-
Amsterdam 17.3.5	17.3.2r	17.8.1r[FC2]	-	-
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	-	-

Release	ROMMON Version (C9300 Models)	ROMMON Version (C9300L Models)	ROMMON Version (C9300X Models)	ROMMON Version (C9300LM Models)
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]	-	-

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 17.3.8a	CAT9K_IOSXE	cat9k_iosxe.17.03.08a.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.08a.SP
Cisco IOS XE Amsterdam 17.3.8	CAT9K_IOSXE	cat9k_iosxe.17.03.08.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.08.SPA
Cisco IOS XE Amsterdam 17.3.7	CAT9K_IOSXE	cat9k_iosxe.17.03.07.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.07.SPA

Release	Image Type	File Name
Cisco IOS XE Amsterdam 17.3.6	CAT9K_IOSXE	cat9k_iosxe.17.03.06.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.06.
Cisco IOS XE Amsterdam 17.3.5	CAT9K_IOSXE	cat9k_iosxe.17.03.05.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.05.
Cisco IOS XE Amsterdam 17.3.4	CAT9K_IOSXE	cat9k_iosxe.17.03.04.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.04.
Cisco IOS XE Amsterdam 17.3.3	CAT9K_IOSXE	cat9k_iosxe.17.03.03.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.03.
Cisco IOS XE Amsterdam 17.3.2a	CAT9K_IOSXE	cat9k_iosxe.17.03.02a.SPA
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.02a
Cisco IOS XE Amsterdam 17.3.1	CAT9K_IOSXE	cat9k_iosxe.17.03.01.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.01.

Upgrading the ROMMON

To know the ROMMON or bootloader version that applies to every major and maintenance release, see ROMMON Versions, on page 21.

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.

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
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 17.3.x
Cisco IOS XE Everest 16.6.2 and all later releases	Either **install** commands or **request platform software** commands[5].	

[5] 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 Amsterdam 17.2.1 to Cisco IOS XE Amsterdam 17.3.1 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 Mon Jul 20 19:51:48 PDT 2020
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
    cat9k-cc_srdriver.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-espbase.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-guestshell.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpbase.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpboot.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipbase.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipspa.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-srdriver.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-webui.17.02.01.SPA.pkg
```

```
      File is in use, will not delete.
    cat9k-wlc.17.02.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.
The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.17.01.01.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 20 19:52:25 PDT 2020
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.17.03.01.SPA.bin flash:
destination filename [cat9k_iosxe.17.03.01.SPA.bin]?
Accessing tftp://10.8.0.6/image/cat9k_iosxe.17.03.01.SPA.bin...
Loading /cat9k_iosxe.17.03.01.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 20 2020 10:18:11 -07:00 cat9k_iosxe.17.03.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

Step 3 Set boot variable

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

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

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

b) **no boot manual**

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

```
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 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.17.03.01.SPA.bin activate commit`.

The following sample output displays installation of the Cisco IOS XE Amsterdam 17.3.1 software image in the flash memory:

```
Switch# install add file flash:cat9k_iosxe.17.03.01.SPA.bin activate commit

install_add_activate_commit: START Mon Jul 20 15:37:20 PDT 2020
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting initial file syncing ---
[2]: Copying flash:cat9k_iosxe.17.03.01.SPA.bin from switch 2 to switch 1 3 4
[1 3 4]: Finished copying to switch 1 switch 3 switch 4
Info: Finished copying flash:cat9k_iosxe.17.03.01.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
  [2] Add package(s) on switch 2
  [2] Finished Add on switch 2
  [3] Add package(s) on switch 3
  [3] Finished Add on switch 3
  [4] Add package(s) on switch 4
  [4] Finished Add on switch 4
Checking status of Add on [1 2 3 4]
Add: Passed on [1 2 3 4]
Finished Add

Image added. Version: 17.03.01
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.03.01.SPA.pkg
/flash/cat9k-webui.17.03.01.SPA.pkg
/flash/cat9k-srdriver.17.03.01.SPA.pkg
/flash/cat9k-sipspa.17.03.01.SPA.pkg
/flash/cat9k-sipbase.17.03.01.SPA.pkg
/flash/cat9k-rpboot.17.03.01.SPA.pkg
/flash/cat9k-rpbase.17.03.01.SPA.pkg
/flash/cat9k-lni.17.03.01.SPA.pkg
/flash/cat9k-guestshell.17.03.01.SPA.pkg
/flash/cat9k-espbase.17.03.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.03.01.SPA.pkg
--- 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.17.02.01.SPA.pkg
      Removed cat9k-espbase.17.02.01.SPA.pkg
      Removed cat9k-guestshell.17.02.01.SPA.pkg
      Removed cat9k-rpbase.17.02.01.SPA.pkg
      Removed cat9k-rpboot.17.02.01.SPA.pkg
      Removed cat9k-sipbase.17.02.01.SPA.pkg
      Removed cat9k-sipspa.17.02.01.SPA.pkg
      Removed cat9k-srdriver.17.02.01.SPA.pkg
      Removed cat9k-webui.17.02.01.SPA.pkg
      Removed cat9k-wlc.17.02.01.SPA.pkg
    New files list:
      Added cat9k-cc_srdriver.17.03.01.SPA.pkg
      Added cat9k-espbase.17.03.01.SPA.pkg
      Added cat9k-guestshell.17.03.01.SPA.pkg
      Added cat9k-lni.17.03.01.SPA.pkg
      Added cat9k-rpbase.17.03.01.SPA.pkg
```

```
    Added cat9k-rpboot.17.03.01.SPA.pkg
    Added cat9k-sipbase.17.03.01.SPA.pkg
    Added cat9k-sipspa.17.03.01.SPA.pkg
    Added cat9k-srdriver.17.03.01.SPA.pkg
    Added cat9k-webui.17.03.01.SPA.pkg
    Added cat9k-wlc.17.03.01.SPA.pkg
  Finished list of software package changes
[1] Finished Activate on switch 1
[2] Activate package(s) on switch 2
  --- Starting list of software package changes ---
  Old files list:
    Removed cat9k-cc_srdriver.17.02.01.SPA.pkg
    Removed cat9k-espbase.17.02.01.SPA.pkg
    Removed cat9k-guestshell.17.02.01.SPA.pkg
    Removed cat9k-rpbase.17.02.01.SPA.pkg
    Removed cat9k-rpboot.17.02.01.SPA.pkg
    Removed cat9k-sipbase.17.02.01.SPA.pkg
    Removed cat9k-sipspa.17.02.01.SPA.pkg
    Removed cat9k-srdriver.17.02.01.SPA.pkg
    Removed cat9k-webui.17.02.01.SPA.pkg
    Removed cat9k-wlc.17.02.01.SPA.pkg
  New files list:
    Added cat9k-cc_srdriver.17.03.01.SPA.pkg
    Added cat9k-espbase.17.03.01.SPA.pkg
    Added cat9k-guestshell.17.03.01.SPA.pkg
    Added cat9k-lni.17.03.01.SPA.pkg
    Added cat9k-rpbase.17.03.01.SPA.pkg
    Added cat9k-rpboot.17.03.01.SPA.pkg
    Added cat9k-sipbase.17.03.01.SPA.pkg
    Added cat9k-sipspa.17.03.01.SPA.pkg
    Added cat9k-srdriver.17.03.01.SPA.pkg
    Added cat9k-webui.17.03.01.SPA.pkg
    Added cat9k-wlc.17.03.01.SPA.pkg
  Finished list of software package changes
[2] Finished Activate on switch 2
[3] Activate package(s) on switch 3
  --- Starting list of software package changes ---
  Old files list:
    Removed cat9k-cc_srdriver.17.02.01.SPA.pkg
    Removed cat9k-espbase.17.02.01.SPA.pkg
    Removed cat9k-guestshell.17.02.01.SPA.pkg
    Removed cat9k-rpbase.17.02.01.SPA.pkg
    Removed cat9k-rpboot.17.02.01.SPA.pkg
    Removed cat9k-sipbase.17.02.01.SPA.pkg
    Removed cat9k-sipspa.17.02.01.SPA.pkg
    Removed cat9k-srdriver.17.02.01.SPA.pkg
    Removed cat9k-webui.17.02.01.SPA.pkg
    Removed cat9k-wlc.17.02.01.SPA.pkg
  New files list:
    Added cat9k-cc_srdriver.17.03.01.SPA.pkg
    Added cat9k-espbase.17.03.01.SPA.pkg
    Added cat9k-guestshell.17.03.01.SPA.pkg
    Added cat9k-lni.17.03.01.SPA.pkg
    Added cat9k-rpbase.17.03.01.SPA.pkg
    Added cat9k-rpboot.17.03.01.SPA.pkg
    Added cat9k-sipbase.17.03.01.SPA.pkg
    Added cat9k-sipspa.17.03.01.SPA.pkg
    Added cat9k-srdriver.17.03.01.SPA.pkg
    Added cat9k-webui.17.03.01.SPA.pkg
    Added cat9k-wlc.17.03.01.SPA.pkg
  Finished list of software package changes
[3] Finished Activate on switch 3
[4] Activate package(s) on switch 4
  --- Starting list of software package changes ---
```

```
    Old files list:
      Removed cat9k-cc_srdriver.17.02.01.SPA.pkg
      Removed cat9k-espbase.17.02.01.SPA.pkg
      Removed cat9k-guestshell.17.02.01.SPA.pkg
      Removed cat9k-rpbase.17.02.01.SPA.pkg
      Removed cat9k-rpboot.17.02.01.SPA.pkg
      Removed cat9k-sipbase.17.02.01.SPA.pkg
      Removed cat9k-sipspa.17.02.01.SPA.pkg
      Removed cat9k-srdriver.17.02.01.SPA.pkg
      Removed cat9k-webui.17.02.01.SPA.pkg
      Removed cat9k-wlc.17.02.01.SPA.pkg
    New files list:
      Added cat9k-cc_srdriver.17.03.01.SPA.pkg
      Added cat9k-espbase.17.03.01.SPA.pkg
      Added cat9k-guestshell.17.03.01.SPA.pkg
      Added cat9k-lni.17.03.01.SPA.pkg
      Added cat9k-rpbase.17.03.01.SPA.pkg
      Added cat9k-rpboot.17.03.01.SPA.pkg
      Added cat9k-sipbase.17.03.01.SPA.pkg
      Added cat9k-sipspa.17.03.01.SPA.pkg
      Added cat9k-srdriver.17.03.01.SPA.pkg
      Added cat9k-webui.17.03.01.SPA.pkg
      Added cat9k-wlc.17.03.01.SPA.pkg
    Finished list of software package changes
  [4] Finished Activate on switch 4
Checking status of Activate on [1 2 3 4]
Activate: Passed on [1 2 3 4]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
  [1] Commit package(s) on switch 1
  [1] Finished Commit on switch 1
  [2] Commit package(s) on switch 2
  [2] Finished Commit on switch 2
  [3] Commit package(s) on switch 3
  [3] Finished Commit on switch 3
  [4] Commit package(s) on switch 4
  [4] Finished Commit on switch 4
Checking status of Commit on [1 2 3 4]
Commit: Passed on [1 2 3 4]
Finished Commit

Send model notification for install_add_activate_commit before reload
[1 2 3 4]: Performing Upgrade_Service

*Jul 20 15:47:28.095: %IOSXEBOOT-4-BOOTLOADER_UPGRADE: (local/local): Starting boot preupgrade
300+0 records in
300+0 records out
307200 bytes (307 kB, 300 KiB) copied, 0.315817 s, 973 kB/s

AppGigabitEthernet port has the latest Firmware

MM [1] MCU version 191 sw ver 196
MM [2] MCU version 191 sw ver 196

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 ...440976 bytes.
Front-end Microcode IMG MGR: Programming device 0...rwRrrrrrrw..
0%.....................................................................................10%
  .....................................................................................20%
  .....................................................................................30%
  .....................................................................................40%
  .....................................................................................50%
  .....................................................................................60%
  .....................................................................................70%
  .....................................................................................80%
  .....................................................................................90%
  .....................................................................................100%
Front-end Microcode IMG MGR: Preparing to program device[0], index=2 ...24506 bytes.
Front-end Microcode IMG MGR: Programming device
0...rrrrrrw..0%....10%....20%......30%...40%....50%......60%....70%.....80%....90%....100%w
Wating for MCU to come up .....Rr!
Front-end Microcode IMG MGR: Microcode programming complete for device 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 298 seconds


MCU UPGRADE COMPLETED!!...  SUCCESS: Upgrade_Service finished
Install will reload the system now!
SUCCESS: install_add_activate_commit  Mon Jul 20 15:52:33 PDT 2020
Switch#
Chassis 2 reloading, reason - Reload command
Jul 20 15:52:36.588: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
Jul 20 15:52:38.199: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes
 exit with reload switch code



Initializing Hardware......

System Bootstrap, Version 17.3.1r[FC2], RELEASE SOFTWARE (P)
Compiled Wed 04/29/2020 12:55:25.08 by rel

Current ROMMON image : Primary
Last reset cause     : SoftwareReload
C9300-48P 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 2
<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 31 2020 09:52:41 -07:00 cat9k-cc_srdriver.17.02.01.SPA.pkg
475141 -rw- 70333380   Mar 31 2020 09:52:44 -07:00 cat9k-espbase.17.02.01.SPA.pkg
475142 -rw- 13256         Mar 31 2020 09:52:44 -07:00 cat9k-guestshell.17.02.01.SPA.pkg
475143 -rw- 349635524 Mar 31 2020 09:52:54 -07:00 cat9k-rpbase.17.02.01.SPA.pkg
475149 -rw- 24248187   Mar 31 2020 09:53:02 -07:00 cat9k-rpboot.17.02.01.SPA.pkg
475144 -rw- 25285572   Mar 31 2020 09:52:55 -07:00 cat9k-sipbase.17.02.01.SPA.pkg
475145 -rw- 20947908   Mar 31 2020 09:52:55 -07:00 cat9k-sipspa.17.02.01.SPA.pkg
475146 -rw- 2962372     Mar 31 2020 09:52:56 -07:00 cat9k-srdriver.17.02.01.SPA.pkg
475147 -rw- 13284288   Mar 31 2020 09:52:56 -07:00 cat9k-webui.17.02.01.SPA.pkg
475148 -rw- 13248         Mar 31 2020 09:52:56 -07:00 cat9k-wlc.17.02.01.SPA.pkg

491524 -rw- 25711568   Jul 20 2020 11:49:33 -07:00 cat9k-cc_srdriver.17.03.01.SPA.pkg
491525 -rw- 78484428   Jul 20 2020 11:49:35 -07:00 cat9k-espbase.17.03.01.SPA.pkg
491526 -rw- 1598412     Jul 20 2020 11:49:35 -07:00 cat9k-guestshell.17.03.01.SPA.pkg
491527 -rw- 404153288 Jul 20 2020 11:49:47 -07:00 cat9k-rpbase.17.03.01.SPA.pkg
491533 -rw- 31657374   Jul 20 2020 11:50:09 -07:00 cat9k-rpboot.17.03.01.SPA.pkg
491528 -rw- 27681740   Jul 20 2020 11:49:48 -07:00 cat9k-sipbase.17.03.01.SPA.pkg
491529 -rw- 52224968   Jul 20 2020 11:49:49 -07:00 cat9k-sipspa.17.03.01.SPA.pkg
491530 -rw- 31130572   Jul 20 2020 11:49:50 -07:00 cat9k-srdriver.17.03.01.SPA.pkg
491531 -rw- 14783432   Jul 20 2020 11:49:51 -07:00 cat9k-webui.17.03.01.SPA.pkg
491532 -rw- 9160           Jul 20 2020 11:49:51 -07:00 cat9k-wlc.17.03.01.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.17.03.01.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 20 2020 10:59:16 -07:00 packages.conf
516098 -rw- 7406 Jul 20 2020 10:58:08 -07:00 cat9k_iosxe.17.03.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

Step 6 Upgrade the ROMMON version

upgrade rom-monitor capsule golden switch

A new ROMMON version is available in Cisco IOS XE Amsterdam 17.3.1, for only the C9300 models in the series. After you enter the command, confirm upgrade at the system prompt.

```
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>
```

For more information about this, see Upgrading the ROMMON, on page 23 in this document.

Step 7 Reload and verify version

a) **reload**

Use this command to reload the switch. When the switch reloads after a ROMMON upgrade, the ROMMON version is updated, but not displayed in the output until the next reload.

```
Switch# reload
```

b) **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 Amsterdam 17.3.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.03.01
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.3.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 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 Amsterdam 17.3.x	Either **install** commands or **request platform software** command[6].	Cisco IOS XE Amsterdam 17.2.x or earlier releases.

[6] 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 Amsterdam 17.3.1 to Cisco IOS XE Amsterdam 17.2.1, 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 20 19:51:48 PDT 2020
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat9k-cc_srdriver.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-espbase.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-guestshell.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpbase.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpboot.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipbase.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipspa.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-srdriver.17.03.01.SSA.pkg
```

```
      File is in use, will not delete.
    cat9k-webui.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-wlc.17.03.01.SSA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.
SUCCESS: No extra package or provisioning files found on media. Nothing to clean.

SUCCESS: install_remove  Mon Jul 20 11:42:39 PDT 2020
```

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.17.02.01.SPA.bin flash:
Destination filename [cat9k_iosxe.17.02.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.17.02.01.SPA.bin...
Loading /cat9k_iosxe.17.02.01.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 20 2020 13:35:16 -07:00 cat9k_iosxe.17.02.01.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.17.03.01.SPA.bin activate commit`.

The following example displays the installation of the Cisco IOS XE Amsterdam 17.2.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.17.02.01.SPA.bin activate commit
install_add_activate_commit: START Mon Jul 20 14:59:46 PDT 2020
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting initial file syncing ---
[1]: Copying flash:cat9k_iosxe.17.02.01.SPA.bin from switch 1 to switch 2 3 4
[2 3 4]: Finished copying to switch 2 switch 3 switch 4
Info: Finished copying flash:cat9k_iosxe.17.02.01.SPA.bin to the selected switch(es)
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
^[[A  [1] Add package(s) on switch 1
  [1] Finished Add on switch 1
  [2] Add package(s) on switch 2
  [2] Finished Add on switch 2
  [3] Add package(s) on switch 3
  [3] Finished Add on switch 3
  [4] Add package(s) on switch 4
  [4] Finished Add on switch 4
Checking status of Add on [1 2 3 4]
Add: Passed on [1 2 3 4]
Finished Add

Image added. Version: 17.02.01.0.306
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.02.01.SPA.pkg
/flash/cat9k-webui.17.02.01.SPA.pkg
/flash/cat9k-srdriver.17.02.01.SPA.pkg
/flash/cat9k-sipspa.17.02.01.SPA.pkg
/flash/cat9k-sipbase.17.02.01.SPA.pkg
/flash/cat9k-rpboot.17.02.01.SPA.pkg
/flash/cat9k-rpbase.17.02.01.SPA.pkg
/flash/cat9k-guestshell.17.02.01.SPA.pkg
```

```
/flash/cat9k-espbase.17.02.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.02.01.SPA.pkg
--- 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.17.03.01.SPA.pkg
      Removed cat9k-espbase.17.03.01.SPA.pkg
      Removed cat9k-guestshell.17.03.01.SPA.pkg
      Removed cat9k-lni.17.03.01.SPA.pkg
      Removed cat9k-rpbase.17.03.01.SPA.pkg
      Removed cat9k-rpboot.17.03.01.SPA.pkg
      Removed cat9k-sipbase.17.03.01.SPA.pkg
      Removed cat9k-sipspa.17.03.01.SPA.pkg
      Removed cat9k-srdriver.17.03.01.SPA.pkg
      Removed cat9k-webui.17.03.01.SPA.pkg
      Removed cat9k-wlc.17.03.01.SPA.pkg
    New files list:
      Added cat9k-cc_srdriver.17.02.01.SPA.pkg
      Added cat9k-espbase.17.02.01.SPA.pkg
      Added cat9k-guestshell.17.02.01.SPA.pkg
      Added cat9k-rpbase.17.02.01.SPA.pkg
      Added cat9k-rpboot.17.02.01.SPA.pkg
      Added cat9k-sipbase.17.02.01.SPA.pkg
      Added cat9k-sipspa.17.02.01.SPA.pkg
      Added cat9k-srdriver.17.02.01.SPA.pkg
      Added cat9k-webui.17.02.01.SPA.pkg
      Added cat9k-wlc.17.02.01.SPA.pkg
    Finished list of software package changes
  [1] Finished Activate on switch 1
  [2] Activate package(s) on switch 2
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k-cc_srdriver.17.03.01.SPA.pkg
      Removed cat9k-espbase.17.03.01.SPA.pkg
      Removed cat9k-guestshell.17.03.01.SPA.pkg
      Removed cat9k-lni.17.03.01.SPA.pkg
      Removed cat9k-rpbase.17.03.01.SPA.pkg
      Removed cat9k-rpboot.17.03.01.SPA.pkg
      Removed cat9k-sipbase.17.03.01.SPA.pkg
      Removed cat9k-sipspa.17.03.01.SPA.pkg
      Removed cat9k-srdriver.17.03.01.SPA.pkg
      Removed cat9k-webui.17.03.01.SPA.pkg
      Removed cat9k-wlc.17.03.01.SPA.pkg
    New files list:
      Added cat9k-cc_srdriver.17.02.01.SPA.pkg
      Added cat9k-espbase.17.02.01.SPA.pkg
      Added cat9k-guestshell.17.02.01.SPA.pkg
      Added cat9k-rpbase.17.02.01.SPA.pkg
      Added cat9k-rpboot.17.02.01.SPA.pkg
      Added cat9k-sipbase.17.02.01.SPA.pkg
      Added cat9k-sipspa.17.02.01.SPA.pkg
      Added cat9k-srdriver.17.02.01.SPA.pkg
      Added cat9k-webui.17.02.01.SPA.pkg
      Added cat9k-wlc.17.02.01.SPA.pkg
    Finished list of software package changes
  [2] Finished Activate on switch 2
  [3] Activate package(s) on switch 3
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k-cc_srdriver.17.03.01.SPA.pkg
      Removed cat9k-espbase.17.03.01.SPA.pkg
      Removed cat9k-guestshell.17.03.01.SPA.pkg
```

```
      Removed cat9k-lni.17.03.01.SPA.pkg
      Removed cat9k-rpbase.17.03.01.SPA.pkg
      Removed cat9k-rpboot.17.03.01.SPA.pkg
      Removed cat9k-sipbase.17.03.01.SPA.pkg
      Removed cat9k-sipspa.17.03.01.SPA.pkg
      Removed cat9k-srdriver.17.03.01.SPA.pkg
      Removed cat9k-webui.17.03.01.SPA.pkg
      Removed cat9k-wlc.17.03.01.SPA.pkg
    New files list:
      Added cat9k-cc_srdriver.17.02.01.SPA.pkg
      Added cat9k-espbase.17.02.01.SPA.pkg
      Added cat9k-guestshell.17.02.01.SPA.pkg
      Added cat9k-rpbase.17.02.01.SPA.pkg
      Added cat9k-rpboot.17.02.01.SPA.pkg
      Added cat9k-sipbase.17.02.01.SPA.pkg
      Added cat9k-sipspa.17.02.01.SPA.pkg
      Added cat9k-srdriver.17.02.01.SPA.pkg
      Added cat9k-webui.17.02.01.SPA.pkg
      Added cat9k-wlc.17.02.01.SPA.pkg
    Finished list of software package changes
  [3] Finished Activate on switch 3
  [4] Activate package(s) on switch 4
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k-cc_srdriver.17.03.01.SPA.pkg
      Removed cat9k-espbase.17.03.01.SPA.pkg
      Removed cat9k-guestshell.17.03.01.SPA.pkg
      Removed cat9k-lni.17.03.01.SPA.pkg
      Removed cat9k-rpbase.17.03.01.SPA.pkg
      Removed cat9k-rpboot.17.03.01.SPA.pkg
      Removed cat9k-sipbase.17.03.01.SPA.pkg
      Removed cat9k-sipspa.17.03.01.SPA.pkg
      Removed cat9k-srdriver.17.03.01.SPA.pkg
      Removed cat9k-webui.17.03.01.SPA.pkg
      Removed cat9k-wlc.17.03.01.SPA.pkg
    New files list:
      Added cat9k-cc_srdriver.17.02.01.SPA.pkg
      Added cat9k-espbase.17.02.01.SPA.pkg
      Added cat9k-guestshell.17.02.01.SPA.pkg
      Added cat9k-rpbase.17.02.01.SPA.pkg
      Added cat9k-rpboot.17.02.01.SPA.pkg
      Added cat9k-sipbase.17.02.01.SPA.pkg
      Added cat9k-sipspa.17.02.01.SPA.pkg
      Added cat9k-srdriver.17.02.01.SPA.pkg
      Added cat9k-webui.17.02.01.SPA.pkg
      Added cat9k-wlc.17.02.01.SPA.pkg
    Finished list of software package changes
  [4] Finished Activate on switch 4
Checking status of Activate on [1 2 3 4]
Activate: Passed on [1 2 3 4]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
  [1] Commit package(s) on switch 1
  [1] Finished Commit on switch 1
  [2] Commit package(s) on switch 2
  [2] Finished Commit on switch 2
  [3] Commit package(s) on switch 3
  [3] Finished Commit on switch 3
  [4] Commit package(s) on switch 4
  [4] Finished Commit on switch 4
Checking status of Commit on [1 2 3 4]
Commit: Passed on [1 2 3 4]
```

```
Finished Commit

Send model notification for install_add_activate_commit before reload
[1 2 3 4]: Performing Upgrade_Service
300+0 records in
300+0 records out
307200 bytes (307 kB, 300 KiB) copied, 0.316195 s, 972 kB/s
MM [1] MCU version 196 sw ver 191
MM [2] MCU version 196 sw ver 191

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 ...440688 bytes.
Front-end Microcode IMG MGR: Programming device 0...rwRrrrrrrw
..0%.....................................................................................10%
    .....................................................................................20%
    .....................................................................................30%
    .....................................................................................40%
    .....................................................................................50%
    .....................................................................................60%
    .....................................................................................70%
    .....................................................................................80%
    .....................................................................................90%
    ....................................................................................100%

Front-end Microcode IMG MGR: Preparing to program device[0], index=2 ...24506 bytes.
Front-end Microcode IMG MGR: Programming device
0...rrrrrrw..0%....10%....20%......30%...40%....50%......60%....70%.....80%....90%....100%w
Wating for MCU to come up .....Rr!
Front-end Microcode IMG MGR: Microcode programming complete for device 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 295 seconds

MCU UPGRADE COMPLETED!!...  SUCCESS: Upgrade_Service finished

Install will reload the system now!
SUCCESS: install_add_activate_commit  Mon Jul 20 15:14:57 PDT 2020
stack-4mnyq#
Chassis 1 reloading, reason - Reload command
Jul 20 15:15:01.382: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
Jul 20 15:15:03.101: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes
 exit with reload switch code

Initializing Hardware......

System Bootstrap, Version 17.3.1r[FC2], RELEASE SOFTWARE (P)
Compiled Wed 04/29/2020 12:55:25.08 by rel

Current ROMMON image : Primary
Last reset cause     : SoftwareReload
C9300-24UX platform with 8388608 Kbytes of main memory

switch: boot
```

```
boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf
#
##################################################################################################################
##################################################################################################################
##################################################################################################################


Waiting for 120 seconds for other switches to boot
Switch is in STRAGGLER mode, waiting for active Switch to boot
Active Switch has booted up, starting discovery phase

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

Switch console is now available

Press RETURN to get started.
```

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 Amsterdam 17.2.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.02.01
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.2.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 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. The version is not downgraded when you downgrade the software image.

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.

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

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

License Levels - Usage Guidelines

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

Smart Licensing Using Policy	Smart Licensing
• Perpetual: There is no expiration date for such a license. • Subscription: The license is valid only until a certain date (for a three, five, or seven year period).	• Permanent: for a license level, and without an expiration date. • Term: for a license level, and for a three, five, or seven year period. • Evaluation: a license that is not registered.

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

Table 4: 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

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.
- 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).
- 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.

- HTTP Services Restriction—If you configure **ip http active-session-modules none** and **ip http secure-active-session-modules none** commands, NGINX process will be held down. This will prevent HTTP or HTTPS from running. Use the **ip http session-module-list** command to enable the required HTTP modules.

- 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 17.3.x

Identifier	Description
CSCvu15010	CMAND crash on 9300 FIAB

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.8a

Identifier	Description
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.8

There are no resolved caveats in this release.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.7

Identifier	Applicable Models	Description
CSCwc87761	9300L	C9300L PWR-C1-350WAC-P power supply may turn off requiring power cable OIR
CSCwd20481	9300	Command **reload cancel** fails when the system clock changes to a later time in between "reload in x"

Identifier	Applicable Models	Description
CSCwd78924	9300	Cat9300 | PoE Imax error detected for PD requesting 30W since 17.3.5+
CSCwd99665	9300L	C9300L-48UXG-4X: TMPFS leak due to excessive logging to debug_logging_file

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.6

Identifier	Description
CSCvx38149	Switch crash while removing private vlan mapping from port-channel interface.
CSCvz36138	It is possible to successfully stack C9300L switches with no Stack Adapters installed
CSCwa00143	C9300 Rcv-Err counter keeps increasing on unused ports
CSCwa10331	Cat9300-48UX ports may not link up when connected to peer Intel NIC I219
CSCwa52014	CISCO-ENHANCED-MEMPOOL-MIB not working on C9200 and C9300
CSCwa57656	C9300 Rcv-Err counter keeps increasing on connected to other non-mgig devices
CSCwa93776	Few ip phones connected to c9300-mGig switches unable to link up if "no mdix auto" is configured
CSCwb18988	some notification-type is missing for "snmp-server host xxx" command

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.5

Identifier	Description
CSCvs33050	SVL Hung - CPU HOG by Process - "Crimson Flush Transaction"
CSCvx38654	Memory leakage is getting incremented whenever dnac-ca crl fails
CSCvy17654	c9300L // SFP-H10GB-CU1M // port stays up/up even if remote side is down
CSCvy40384	Cat9300L: 1G SFP uplink does not come up after reload
CSCvy51582	SNMP: sub-interface octet counter reports wrong value
CSCvz01398	Incorrect L3 LISP instance ID on Cef table for VN's
CSCvz32969	Cat9k | DHCP unicast ACK not forwarded to the client when DHCP snooping is enabled
CSCvz54210	C9300 / C9500 / C9500H // Constraining Uncore Frequency on CPU to mitigate Hang/Crash
CSCvz78724	Reload at unable to access memory address of "swmd"

Identifier	Description
CSCvz85562	Link may not come up between C9300 and C9500 at 25G with SFP-10/25G-CSR-S
CSCvz89443	BinOS: linux_iosd-imag_rp_0 memory leak with chasfs_ctx_int_t upon insert/remove events in PM

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.4

Identifier	Description
CSCvt34738	SVL // DHCP discover relayed in a different vlan
CSCvv82819	Manually configured MAC address is programmed in hardware when interface is admin down
CSCvv97807	Netconf & Netconf-yang are not enabled on the Ext-Nodes as part of PnP config.
CSCvv97823	Yang requests from DNAC to IoT devices related to device Licensing are failing on the device
CSCvw13923	Vlan randomly stop forwarding DHCP pkts - Wedged input interface queue
CSCvw32545	STACK : Stale mac entry in the member switch causing the connectivity issues.
CSCvw51810	Disruption of IP communication due to AUTH_DRIVEN_DROP on uplinks when flapping downlink ports
CSCvx06374	Profinet (PN-PTCP) frames overwhelming L2 Control CoPP queue on Cat9K
CSCvx11287	9300L - No connectivity when using GLC-LH-SMD on uplinks with speed nonegotiate on both ends
CSCvx15864	ETA+AVC: After active timer expiry, multiple FNF exports sent for same flow
CSCvx25344	Private Native Vlan packets are erroneously tagged
CSCvx25489	GLC-BX-U SFP transceiver not recognized on C9300L
CSCvx25841	DHCP snooping trust state breaks when there is change in REP segment
CSCvx29670	Memory leak due to .nvram_config file creation under TAM
CSCvx60124	Traffic failed if incoming interface MPLS and 2+ outgoing interfaces (ECMP) with recursive routing
CSCvx83266	DHCP snooping and PVLAN dropping DHCP Offer unicast packet on C9K
CSCvx87277	Cat9XXX may experience an unexpected reboot with Critical process fed fault on fp_0_0
CSCvx90075	9300-NM-8X + SFP-H10GB-CU 3m or 5m and certain link partners could experience long link times

Identifier	Description
CSCvx94722	Radius protocol generate jumbo frames for dot1x packets
CSCvx95451	Switch stack crash with FIPS mode enabled
CSCvx96576	C9300 switches incorrectly log %THERMAL-1-THERMAL_GREEN_THRESHOLD: Switch 1 R0/0:
CSCvy02075	Switch forwards traffic received on ports in blocking BLK state
CSCvy07376	Catalyst 9K Switch may crash on ISSU upgrade if run debug issu all

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.3

Identifier	Description
CSCvr77861	Cat9300/C9500/C9500H switches may reload with last reload reason as LocalSoft or CpuCatastrophicErr
CSCvt73669	Ports remains in notconnect state when moved from L2 to L3 to L2
CSCvu14969	DNAC SWIM \"in-progress\" due to underline SNMPwalk timesout after upgrade to image
CSCvu38231	Configuring reserved PO 127 & 128 in SVL setup disables show etherchannel CLI
CSCvu54327	User can config up to 255 vrf instead of 256 vrfs
CSCvu90016	Catalyst 9k: FED crash after reaching webauth scale of about 1k sessions
CSCvv26018	Loopback error is not detected on trunk interface
CSCvv27849	Unexpected reload caused by the FED process.
CSCvv39593	'SL using Policy' to SL downgrade to 16.12.4 leads to \"Initial Registration-First Attempt Pending\"
CSCvv56278	Dot1x Client mac in dropped state post switchover
CSCvv88670	[SDA] SISF marking mac as tentative
CSCvw09998	flexlink+ alt port forwarding igmp queries caused multicast traffic loop
CSCvw18461	Switch Crashes when enabling RSPAN Destination port
CSCvw19588	Higher Traffic down time observed during reload fast with C9300-NM-4M FRU
CSCvw20225	Cat9k switches may roll back to old software after unexpected switchover event
CSCvw23637	SNMP reports wrong octets received or transmitted value for portchannel subinterfaces
CSCvw28418	VRF leaking using self-GRE tunnels causes traffic to be punted to CPU.
CSCvw32481	EVPN Type-2 IP/MAC route is created for not-connected SVI

Identifier	Description
CSCvw65866	Packet loss and jitter seen for media traffic when connected to C9300-48UN
CSCvw73903	Some SFP's on Cat9300S downlink port does not come up after power cycle
CSCvw74061	Cat9300 & Cat9500 series switches may see unexpected reloads due to Localsoft or CpuCatastrophicErr
CSCvw84422	C9K || A hosted application does not start after reboot when usbflash1/SSD is secured with password
CSCvw87096	Cat9300 interface remains down after a reload of an individual stack member
CSCvx34691	Appgig port not present on C9300-48H SKU

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.2a

Identifier	Description
CSCvq13832	Whenever Acct-terminate-cause is 24 the duplicate set of traffic counts is sent as 0.
CSCvt18739	Cat9K - incorrect source mac address used for L3 packets after L3 link flap
CSCvt70277	Power allocation issue in 16.9.x/16.12.x
CSCvt93918	Cat9k reboot due to ACL count being huge.
CSCvt95680	Unexpected Reload when a VLAN is created within the range 2-1002
CSCvu25094	9300L crash due "stack cable authentication failure" reload reason only once
CSCvu25931	DHCPv6 RELAY-REPLY dropped when punted on cat9k
CSCvu52246	sessmgrd memory leak when CTS PAC download fails
CSCvu62273	CLI should be auto-upgraded from "tacacs-server" cli to newer version while upgrading
CSCvu65433	Cat9300 stack member 'platform_mgr' process crash on obfl poe sensor handler
CSCvu82477	Random L3 ports stop traffic processing on SDA internal border nodes
CSCvu90882	Switch might enter a bootloop with SWITCH_DISABLE_PASSWORD_RECOVERY & IGNORE_STARTUP_CFG set to 1
CSCvu94010	Cat9k Active stack switch crash while applying the CTS configuration
CSCvv16874	CAT9K: PRD18: SISF Crash seen on device when left traffic running overnight
CSCvv26075	On Auth port, timestamp update is not happening for Authz MAC address upon RX of control-plane/BPDU
CSCvv32161	Traffic is not resuming after Phyloopback test with xMGig uplink connected interface
CSCvv34688	IPv6 communication stops working post applying ipv6 source-guard on interface

Identifier	Description
CSCvv35565	L3 ECMP load balancing not working as expected for fragmented packets.
CSCvv40022	Enable mode button BTN_HELD_XS_5 event
CSCvv44720	IPV4 and IPV6 Per-User ACL is not working together on singe authentication session
CSCvv45801	inconsistent behaviour for autoconf template binding after switchover
CSCvv48305	Route not fully programmed in the hardware for macsec enabled end-point
CSCvv54278	cat9300 - multiple crashes while freeing a buffer in lsmpi
CSCvv69764	Dot1Q Native vlan tag is ignored after configuring Layer2 Vlan on 16.12.4 code
CSCvv77355	Cat9k in VXLAN with directed-broadcast on egress interface duplicates broadcast traffic
CSCvv86246	CAT9K reload due to "Critical process cmand fault on rp_0_0 (rc=139)"

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.1

Identifier	Description
CSCvm08733	Cadyce USB/Serial converter causes C9300 to loop at "Initializing Hardware..."
CSCvr92287	EPC with packet-len opt breaks CPU in-band path for bigger frames
CSCvs15485	Cat9k PoE models - when configuring speed 100 and duplex full on both sides, interface will not come up
CSCvs22896	DHCPv6 RELAY-REPLY packet is being dropped
CSCvs36803	When port security applied mac address not learned on hardware
CSCvs50391	FED crash when premature free of SG element
CSCvs52594	9300L-XX may not provide POE on certain ports after being powered-on
CSCvs71084	Cat9k - Not able to apply Et-analytics on an interface
CSCvs84212	DHCP server sends out a NAK packet during DHCP renewal process.
CSCvs91195	Crash Due to AutoSmart Port Macros
CSCvs97551	Unable to use VLAN range 4084-4095 for any business operations
CSCvt13518	QoS ACL matching incorrectly when udp range is used
CSCvt59448	LACP link suspend or PAgP link getting into error-disabled if stack-mac persistent timer is set
CSCvt60246	C9300L-48T-4X cannot detect PSU oir after fullly booting up.

Identifier	Description
CSCvt99199	MACSEC issue in SDA deployment

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 results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020–2023 Cisco Systems, Inc. All rights reserved.