Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Gibraltar 16.11.x

First Published: 2019-03-29

Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Gibraltar 16.11.x

Introduction

Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance are Cisco's lead, fixed core and aggregation enterprise switching platforms. They have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

They deliver complete convergence in terms of ASIC architecture with Unified Access Data Plane (UADP) 2.0 on Cisco Catalyst 9500 Series Switches and UADP 3.0 on Cisco Catalyst 9500 Series Switches - High Performance. The platform runs an Open Cisco IOS XE that supports model driven programmability, 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.

Note With the introduction of the High Performance models in the series, there may be differences in the supported and unsupported features, limitations, and caveats that apply to the Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance models. Throughout this release note document, any such differences are expressly called out. If they are not, the information applies to all models in the series.

Attention

Important Upgrade Prerequisite for Cisco Catalyst 9500 Series Switches - High Performance

Starting with Cisco IOS XE Gibraltar 16.11.1, the default interface for all High Performance models in the series changes from Layer 3 to Layer 2.

To ensure that this change does not erase existing configuration, complete the task described here: Changing the Default Interface and Upgrading or Downgrading in Install Mode (for Cisco Catalyst 9500 Series Switches - High Performance Only) , on page 21**, *before* you upgrade to or downgrade.**

Whats New in Cisco IOS XE Gibraltar 16.11.1

Hardware Features in Cisco IOS XE Gibraltar 16.11.1

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

Hardware Features Introduced on Cisco Catalyst 9500 Series Switches

(C9500-12Q, C9500-16X, C9500-24Q, C9500-40X)

Feature Name	Description and Documentation Link
Cisco 40GBASE QSFP-40G Modules	Supported transceiver module product number: QSFP-40/100-SRBD **Note** Although this is a dual-rate transceiver module, only the 40G mode is currently supported. For information about the module, see the Cisco 100GBASE QSFP-100G Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.
Cisco 25GBASE SFP28 Modules	Supported transceiver module product numbers: Cisco SFP-10/25G-LR-S For information about the module, see the Cisco 25GBASE SFP28 Modules Data Sheet and Cisco 25G Transceivers and Cables Enable 25 Gigabit Ethernet over a Fiber or Copper Cable. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.
Cisco SFP Modules	Supported transceiver module product numbers: • GLC-SX-MM-RGD • GLC-LX-SM-RGD • GLC-ZX-SM-RGD For information about the module, see the Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

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

(C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C)

Feature Name	Description and Documentation Link
Cisco 100GBASE QSFP-100G Module	• Supported transceiver module product numbers: QSFP-100G-ER4L-S • Compatible switch models: C9500-32C, C9500-32QC, C9500-48Y4C, C9500-24Y4C For information about the module, see the Cisco 100GBASE QSFP-100G Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Cisco 10GBASE SFP+ modules and Cisco SFP+ active optical cables	• Supported transceiver module product numbers:
	  • SFP-10G-SR-X
	  • SFP-10G-LR-X
	• Supported cable product numbers
	  • SFP-H10GB-CU1-5M, SFP-H10GB-CU2-5M
	  • SFP-H10GB-CU2M
	• Compatible switch models: C9500-48Y4C, C9500-24Y4C
	
	For information about the module, see the Cisco 10GBASE SFP+ Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Cisco 25GBASE SFP28 Modules	• Supported transceiver module product numbers: Cisco SFP-10/25G-LR-S • Compatible switch models: C9500-24Y4C and C9500-48Y4C For information about the module, see the Cisco 25GBASE SFP28 Modules Data Sheet and Cisco 25G Transceivers and Cables Enable 25 Gigabit Ethernet over a Fiber or Copper Cable. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Cisco 40GBASE QSFP Modules: Breakout Cables	• Supported transceiver module product numbers:
	  • QSFP-40G-SR4 (10G)
	  • QSFP-40G-SR4-S (10G)
	  • QSFP-40G-CSR4 (10G)
	• Compatible switch models: C9500-32C
	
	For information about the module, and breakout cables see the Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Software Features in Cisco IOS XE Gibraltar 16.11.1

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

Software Features Introduced on All Models

Feature Name	Description, Documentation Link and License Level Information
Cisco StackWise Virtual—Recovery Reload	Introduces a new default reload action after recovering from a link failure and the option to disable this default. Starting with this release, after recovering from a StackWise Virtual link failure, the failed active switch automatically performs a reload action and restores itself as a standby switch. This is the new default behaviour in the event of a link failure. You can also configure the **dual-active recovery-reload-disable** command in the stackwise-virtual configuration mode, to retain the switch in recovery mode and prevent the switch from reloading automatically. See High Availability → Configuring Cisco StackWise Virtual. (Network Advantage)
Consent Token for Shell Access	Authenticates a network administrator's request to access the system shell. When debugging software issues, a Cisco TAC engineer may have to work with a network administrator to collect debug information or perform live debugging on a production system. This feature provides the network administrator with privileged, restricted, and secure access to the system shell with mutual consent from the network administrator and Cisco TAC. See System Management → Consent Token. (Network Essentials and Network Advantage)
Ingress Replication (IR) for VXLAN BGP EVPN	Enables forwarding of broadcast, unknown unicast, and multicast (BUM) traffic to the relevant recipients in a network. IR is a unicast approach to handling multi-destination traffic, and involves an ingress device replicating every BUM packet and then sending it as a separate unicast to remote egress devices. See Layer 2 → Configuring VXLAN BGP EVPN. (Network Advantage)
IPv6 Support for Virtual Extensible LAN (VXLAN) Border Gateway Protocol (BGP) Ethernet VPN (EVPN) in Routed Mode	Introduces IPv6 support for the VXLAN BGP EVPN operation in routed mode. A VXLAN is a network overlay that allows layer 2 segments to be stretched across an IP core. All the benefits of Layer 3 topologies are thereby available with VXLAN. The overlay protocol is VXLAN and BGP uses EVPN as the address family for communicating end host MAC and IP addresses. VXLAN BGP EVPN operates in bridged mode when the hosts are in the same subnet, and in routed mode when the hosts are in different subnets. See Layer 2 → Configuring VXLAN BGP EVPN. (Network Advantage)

Feature Name	Description, Documentation Link and License Level Information
Multiprotocol Label Switching (MPLS) • MPLS VPN-Inter-AS Option B • MPLS VPN-Inter-AS-IPv4 BGP Label Distribution • MPLS over GRE • MPLS VPN eBGP Multipath Support for Inter-AS VPNs	• MPLS VPN-Inter-AS Option B—Allows an MPLS Virtual Private Network (VPN) service provider to interconnect different autonomous systems to provide VPN services. In an Inter-AS Option B network, autonomous system boundary router (ASBR) peers are connected by one or more interfaces that are enabled to receive MPLS traffic. • MPLS VPN-Inter-AS-IPv4 BGP Label Distribution—Enables you to set up a VPN service provider network so that ASBRs exchange IPv4 routes with MPLS labels of the provider edge (PE) routers. • MPLS over GRE—Provides a mechanism for tunneling MPLS packets over non-MPLS networks by creating a generic routing encapsulation (GRE) tunnel. The MPLS packets are encapsulated within the GRE tunnel packets, and the encapsulated packets traverse the non-MPLS network through the GRE tunnel. When GRE tunnel packets are received at the other side of the non-MPLS network, the GRE tunnel packet header is removed and the inner MPLS packet is forwarded to its final destination. • MPLS VPN eBGP Multipath Support for Inter-AS VPNs—Enables you to configure external Border Gateway Protocol (eBGP) multipath with IPv4 labels. It allows load balancing of VPN traffic when you use VPNv4 peering for Inter-AS VPNs. Without this feature, the MPLS forwarding table contains the labels only for the BGP best path even though the routing table has more than one path for the prefix. See Multiprotocol Label Switching. (Network Advantage)
Programmability • Kill Telemetry Subscription • NETCONF and RESTCONF Service Level Access Control Lists • YANG Data Models	The following programmability features are introduced in this release: • Kill Telemetry Subscription—Provides the ability to delete a dynamic model driven telemetry subscription using either: • The **clear telemetry ietf subscription** Cisco IOS command, or • The <kill-subscription> RPC • NETCONF and RESTCONF Service Level Access Control Lists (ACLs)—Enables you to configure an IPv4 or IPv6 ACL for NETCONF and RESTCONF sessions. Clients that do not conform to the configured ACL are not allowed to access the NETCONF or RESTCONF subsystems. When service-level ACLs are configured, NETCONF and RESTCONF connection requests are filtered based on the source IP address. • YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate tohttps://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16111. Revision statements embedded in the YANG files indicate if there has been a model revision. The *README.md* file in the same GitHub location highlights changes that have been made in the release. See Programmability. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link and License Level Information
Smart Licensing: System Messages for an Evaluation License	Evaluation licenses that are not registered will still expire after the 90-day period, but warning system messages about an evaluation license expiry will now be generated only 275 days after this 90-day window. See License Levels - Usage Guidelines, on page 39. (A license level does not apply)

New on the Web UI	
• Application Visibility and Control (AVC) • Switching Database Manager (SDM) templates • Cisco TrustSec	Use the WebUI to: • Configure and monitor AVC—Enables you to configure application-level classification, monitoring, and traffic control. It helps with improved network capacity management, faster troubleshooting, and lower operating costs. Also, Network-Based Application Recognition (NBAR) supports the use of custom protocols to identify customer-specific applications. • Apply SDM templates—Helps configure system resources to optimize support for specific features, depending on how your device is used in the network. • Configure and monitor Cisco TrustSec—Helps build secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

Software Features Introduced on Cisco Catalyst 9500 Series Switches

C9500-12Q, C9500-16X, C9500-24Q, C9500-40X

Feature Name	Description, Documentation Link and License Level Information
BGP PE-CE support for MPLS Layer 3 VPNs	Supports BGP as a routing protocol between the provider edge (PE) device and the customer edge (CE) device. See Configuring MPLS Layer 3 VPN. (Network Advantage)
Cisco StackWise Virtual: Support on uplink network modules	On the C9500-40X and C9500-16X models of the Cisco Catalyst 9500 Series Switches, you can now configure StackWise Virtual links and Dual Active Detection (DAD) links on any of the compatible uplink network modules. For the list of supported network modules, see Network Modules, on page 15. See High Availability → Configuring Cisco StackWise Virtual. (Network Advantage)

Feature Name	Description, Documentation Link and License Level Information
ERSPAN Termination	Introduces support for encapsulated remote switched port analyzer (ERSPAN) type 3 source feature and the following ERSPAN type 2 and type 3 features: • Security group tag (SGT) • Differentiated services code point (DSCP) • Remote SPAN based redirection • Virtual routing and forwarding (VRF) • Termination The **header-type 3**, **destination**, **ip dscp**, **filter mtu**, and **vrf** commands are available for configuration. See Network Management → Configuring ERSPAN. (DNA Advantage)
IPv6: Border Gateway Protocol (BGP)	IPv6 support is introduced for following BGP features: • IPv6: BGP Conditional Route Injection • IPv6: BGP Configuration Using Peer Templates • IPv6: BGP Next Hop Propagation • IPv6: BGP Support for 4-byte ASN See IP Routing.
IPv6: IP Service Level Agreements (SLAs)	IPv6 support is introduced for following IP SLA features: • IPv6: IP SLAs - History Statistics • IPv6: IP SLAs - ICMP Path Echo Operation • IPv6: IP SLAs - UDP Echo Operation See Network Management → Configuring Service Level Agreements. (Network Essentials and Network Advantage)
IPv6: IPv6 Multicast Virtual Private Network (MVPNv6)	Enables service providers to use their existing IPv4 backbone to provide multicast-enabled private IPv6 networks to their customers. See IP Multicast Routing → Configuring Multicast Virtual Private Network (Network Advantage)

Feature Name	Description, Documentation Link and License Level Information
IPv6: Open Shortest Path First (OSPF)	IPv6 support is introduced for following OSPF features: • IPv6: OSPF Forwarding Address Suppression in Translated Type-5 LSAs • IPv6: OSPF Inbound Filtering using Route Maps with a Distribute List • IPv6: OSPF MIB Support of RFC 1850 and Latest Extensions • IPv6: OSPF Stub Router Advertisement • IPv6: OSPF Support for Link State Advertisement (LSA) Throttling • IPv6: OSPF Update Packet-Pacing Configurable Timers See IP Routing. (Network Essentials and Network Advantage)
Password Configuration: Secure Password Migration	Introduces support for migration of type 0 and type 7 usernames and passwords to type 6. Password protection restricts access to a network or network device. Encrypting passwords provides an additional layer of security, particularly for passwords that cross the network or are stored on a TFTP server. Starting with this release, the switch supports automatic conversion of usernames and passwords with type 0 and type 7 encryption, to type 6 encryption. Type-6 is a strong, reversible 128-bit Advanced Encryption Standard (AES) password encryption. To start using type-6 encryption, you must enable the AES password encryption feature and configure a master encryption key, which is used to encrypt and decrypt passwords. See Security → Controlling Switch Access with Passwords and Privilege Levels. (Network Essentials and Network Advantage)

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

C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C

Feature Name	Description, Documentation Link and License Level Information
BFD support for PE-CE, PE-P in an MPLS network	Enables configuration of the BFD protocol between PE-CE (Provider Edge-Customer Edge) and PE-P (Provider Edge- Provider) in an MPLS network. See IP Routing → Configuring Bidirectional Forwarding Detection. (Network Advantage)

Feature Name	Description, Documentation Link and License Level Information
Bidirectional Forwarding Detection (BFD): • BFD Support for GRE IP Tunnel • BFD support for IPv6 BGP Neighbours • BFD Multihop support for IPv4 Static Routes • BFD Support for EIGRP IPv6	BFD is a detection protocol that is designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. BFD provides faster reconvergence time for BGP after a forwarding path failure. Starting with this release: • BFD Support for GRE IP Tunnel—BFD forwarding on point-to-point IPv4, IPv6, and Generic Routing Encapsulation (GRE) tunnels is supported. • BFD support for IPv6 BGP Neighbours—BFD can be used to track fast forwarding path failure of BGP neighbours that have an IPv6 address. • BFD Multihop support for IPv4 Static Routes—BFD multihop support enables detection of IPv4 network failure between paths that are not directly connected. If a BFD session is up, the IPv4 static routes associated with the IPv4 static BFD configuration are added to a routing table. If the session is down, static routes are removed from the routing table. • BFD Support for EIGRP IPv6—BFD support for Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 sessions facilitate rapid fault detection and alternate-path selection in EIGRP IPv6 topologies. See IP Routing. (Network Essentials and Network Advantage)
Etherchannel VLAN Based Load Balancing	Enables you to configure EtherChannel load balancing based on the VLAN IDs of packets. EtherChannels can balance traffic load across links in the channel by reducing part of the binary pattern formed from the addresses or ports in the frame, to a numerical value that selects one of the links in the channel. You can specify one of several different load-balancing modes, which now includes VLAN-based load balancing. The selected mode applies to all EtherChannels configured on the device. See Layer 2 → Configuring EtherChannels. (Network Essentials and Network Advantage)
HSRP V2 - Sub Second Timers	Enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. You can optionally configure an HSRP authentication string or change the hello-time interval and hold time. Starting from this release, the **msec** keyword is supported. We recommend that you configure a minimum hello-time value of 250 milliseconds and a minimum hold-time value of 800 milliseconds. See IP Addressing Services → Configuring HSRP. (Network Essentials and Network Advantage)
IPv6: OSPF Limit on Number of Redistributed Routes	Enables you to configure a maximum number of prefixes (routes) that can be redistributed into OSPFv3 from other protocols or other OSPFv3 processes. Such a limit helps prevent the device from being flooded by too many redistributed routes. See IP Routing → Configuring OSPFv3 Limit on Number of Redistributed Routes. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link and License Level Information
IPv6: RFC 5453 Reserved IPv6 Interface Identifiers	An autoconfigured IPv6 address can contain interface identifiers that are not part of the reserved range of interface identifiers specified in RFC 5453. See IP Multicast Routing → IP Multicast Routing Technology Overview. (Network Essentials and Network Advantage)
IPv6 Downloadable ACL (DACL)	Applies per-port IPv6 access-layer restrictions based on Identity Services Engine (ISE) profiles. See Security → IPv6 ACLs. (Network Essentials and Network Advantage)
IPv6 Neighbor Discovery • Creating global IPv6 entries for unsolicited NA • IPv6 ND cache expire • Option to configure exponential backoff for NS timer used in NUD	• Creating global IPv6 entries for unsolicited neighbor advertisements (NA)—Introduces support for the **ipv6 nd na glean** interface configuration command. This command configures neighbor discovery (ND) to glean an entry from an unsolicited NA. • IPv6 ND cache expire—Introduces support for the **ipv6 nd nud retry** interface configuration command. This command configures neighbor discovery to maintain an neighbor discovery cache entry for a neighbor during network disruption. • Option to configure exponential backoff for neighbor solicitation (NS) timer used in neighbor unreachability detection (NUD)—Introduces support for the **ipv6 nd cache expire refresh** interface configuration command. This command configures the neighbor to maintain an neighbor discovery cache entry, when no traffic is sent to the neighbor. See IP Addressing Services → Enhanced IPv6 Neighbor Discovery Cache Management. (Network Essentials and Network Advantage)
MIBs for IPv6 traffic	The following RFCs are supported: • RFC4292-IP Forwarding Table MIB • RFC4293- Management Information Base for the Internet Protocol (IP) To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at the following URL: http: www.cisco.com go mibs (Network Essentials and Network Advantage)
Multiprotocol Label Switching (MPLS): EIGRP MPLS VPN PE-CE Site of Origin (SoO)	Introduces the capability to filter MPLS Virtual Private Network (VPN) traffic on a per-site basis for Enhanced Interior Gateway Routing Protocol (EIGRP) networks. SoO filtering is configured at the interface level. It is used to manage MPLS VPN traffic and to prevent transient routing loops from occurring in complex and mixed network topologies. See Multiprotocol Label Switching → Configuring EIGRP MPLS VPN PE-CE Site of Origin. (Network Advantage)

Feature Name	Description, Documentation Link and License Level Information
Per-port native VLAN tagging	Provides the option to enable or disable native VLAN tagging on a per-port basis. Normally, you configure 802.1Q trunks with a native VLAN ID, which strips tagging from all packets on that VLAN. To maintain tagging on the native VLAN and drop untagged traffic, use the [**no**] **vlan dot1q tag native** command in global configuration mode. See Layer 2 → Configuring IEEE 802.1Q Tunneling. (Network Essentials and Network Advantage)
Selective Q-in-Q	Maps the specified customer VLAN-IDs (C-VLANs) entering the User Network Interface (UNI) to the specified, translated VLAN IDs (S-VLANs). The feature enables selective tunnelling or translation of C-VLANs to S-VLANs on interfaces configured as trunk ports. The egress packet is double-tagged with the C-VLAN ID and the mapped S-VLAN ID. See Layer 2 → Configuring VLAN Mapping. (Network Essentials and Network Advantage)
VRRPv3 Object Tracking: IPv6 Integration	Virtual Router Redundancy Protocol (VRRP) enables a group of devices to form a single virtual device to provide redundancy. Object tracking is an independent process that manages the creation, monitoring, and removal of tracked objects such as: the state of the line protocol of an interface, the state of an IP route, or the reachability of a route. Clients (like VRRP) register their interest with specific tracked objects and act when the state of an object changes. Starting with this release, the VRRPv3 Object Tracking Integration features supports IPv6. See IP Addressing Services → VRRPv3: Object Tracking Integration. (Network Advantage)

Important Notes

- Cisco StackWise Virtual - Supported and Unsupported Features, on page 11
- Unsupported Features—All Models, on page 12
- Unsupported Features—Cisco Catalyst 9500 Series Switches, on page 12
- Unsupported Features—Cisco Catalyst 9500 Series Switches - High Performance, on page 12
- Complete List of Supported Features, on page 13
- Accessing Hidden Commands, on page 13
- Changing the Default Interface Behaviour—Cisco Catalyst 9500 Series Switches - High Performance Only, on page 14

Cisco StackWise Virtual - Supported and Unsupported Features

(applies only to C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models)

When you enable Cisco StackWise Virtual on the device

- Layer 2, Layer 3, Security, Quality of Service, Multicast, Application, Monitoring and Management, Multiprotocol Label Switching, and High Availability are supported.

  Contact the Cisco Technical Support Centre for the specific list of features that are supported under each one of these technologies.

- Resilient Ethernet Protocol, Remote Switched Port Analyzer, and Sofware-Defined Access are NOT supported

Unsupported Features—All Models

- Bluetooth
- Bidirectional Protocol Independent Multicast (Bidir-PIM)
- IPsec VPN
- Performance Monitoring (PerfMon)
- Virtual Routing and Forwarding (VRF)-Aware web authentication

Unsupported Features—Cisco Catalyst 9500 Series Switches

- Border Gateway Protocol (BGP) Additional Paths
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Flexible NetFlow—NetFlow v5 Export Protocol, 4-byte (32-bit) AS Number Support, TrustSec NetFlow IPv4 Security Group Access Control List (SGACL) Deny and Drop Export
- Gateway Load Balancing Protocol (GLBP)
- Lawful Intercept (LI)
- Network-Powered Lighting (including COAP Proxy Server, 2-event Classification, Perpetual POE, Fast PoE)
- PIM Bidirectional Forwarding Detection (PIM BFD), PIM Snooping.
- Quality of Service—Classification (Layer 3 Packet Length, Time-to-Live (TTL)), per queue policer support, sharped profile enablement for egress per port queues, L2 Miss, Ingress Packet FIFO (IPF)
- Unicast over Point to Multipoint (P2MP) Generic Routing Encapsulation (GRE), Multicast over P2MP GRE.

Unsupported Features—Cisco Catalyst 9500 Series Switches - High Performance

- Cisco Application Visibility and Control (AVC)
- MPLS Label Distribution Protocol (MPLS LDP) VRF-Aware Static Labels
- Next Generation Network-Based Application Recognition (NBAR) and Next Generation NBAR (NBAR2)
- QoS Options on GRE Tunnel Interfaces

Complete List of Supported Features

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

When you search for the list of features by platform select

- CAT9500—to see all the features supported on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models
- CAT9500 HIGH PERFORMANCE (32C; 32QC; 48Y4C; 24Y4C)—to see all the features supported on the C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C models

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. This means that entering enter a question mark (?) at the system prompt did not display the list of available commands. For information about CLI help, see Understanding the Help System. Such hidden commands are only meant to assist Cisco TAC in advanced troubleshooting and are therefore not documented.

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. Entering enter a question mark (?) at the system prompt displays the list of available commands.

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

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

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

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



Important We recommend that you use 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.

Changing the Default Interface Behaviour—Cisco Catalyst 9500 Series Switches - High Performance Only

Starting with Cisco IOS XE Gibraltar 16.11.1, the default interface for all High Performance models in the series changes from Layer 3 to Layer 2.

To ensure that this change does not erase existing configuration, complete the task described here: Changing the Default Interface and Upgrading or Downgrading in Install Mode (for Cisco Catalyst 9500 Series Switches - High Performance Only) , on page 21, *before* you upgrade to or downgrade from Cisco IOS XE Gibraltar 16.11.1.

Supported Hardware

Cisco Catalyst 9500 Series Switches—Model Numbers

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

Base PIDs are the model numbers of the switch.

Bundled PIDs indicate the orderable part numbers for base PIDs that are bundled with a particular network module. Entering the **show version**, **show module**, or **show inventory** commands on such a switch (bundled PID), displays its base PID.

Table 1: Cisco Catalyst 9500 Series Switches

Switch Model	Default License Level	Description
Base PIDs		
C9500-12Q-E	Network Essentials	12 40-Gigabit Ethernet QSFP+ ports and two power supply slots
C9500-12Q-A	Network Advantage	
C9500-16X-E	Network Essentials	16 1/10-Gigabit Ethernet SFP/SFP+ ports and two power supply slots
C9500-16X-A	Network Advantage	
C9500-24Q-E	Network Essentials	24-Port 40-Gigabit Ethernet QSFP+ ports and two power supply slots
C9500-24Q-A	Network Advantage	
C9500-40X-E	Network Essentials	40 1/10-Gigabit Ethernet SFP/SFP+ ports and two power supply slots
C9500-40X-A	Network Advantage	
Bundled PIDs		
C9500-16X-2Q-E	Network Essentials	16 10-Gigabit Ethernet SFP+ port switch and a 2-Port 40-Gigabit Ethernet (QSFP) network module on uplink ports
C9500-16X-2Q-A	Network Advantage	
C9500-24X-E	Network Essentials	16 10-Gigabit Ethernet SFP+ port switch and an 8-Port 10-Gigabit Ethernet (SFP) network module on uplink ports
C9500-24X-A	Network Advantage	

Switch Model	Default License Level	Description
C9500-40X-2Q-E	Network Essentials	40 10-Gigabit Ethernet SFP+ port switch and a 2-Port 40-Gigabit Ethernet (QSFP) network module on uplink ports
C9500-40X-2Q-A	Network Advantage	
C9500-48X-E	Network Essentials	40 10-Gigabit Ethernet SFP+ port switch and an 8-Port 10-Gigabit Ethernet (SFP) network module on uplink ports
C9500-48X-A	Network Advantage	

Table 2: Cisco Catalyst 9500 Series Switches-High Performance

Switch Model	Default License Level	Description
C9500-24Y4C-E	Network Essentials	24 SFP28 ports that support 1/10/25-GigabitEthernet connectivity, four QSFP uplink ports that support 100/40-GigabitEthernet connectivity; two power supply slots.
C9500-24Y4C-A	Network Advantage	
C9500-32C-E	Network Essentials	32 QSFP28 ports that support 40/100 GigabitEthernet connectivity; two power supply slots.
C9500-32C-A	Network Advantage	
C9500-32QC-E	Network Essentials	32 QSFP28 ports, where you can have 24 ports that support 40-GigabitEthernet connectivity and 4 ports that support 100-GigabitEthernet connectivity, OR 32 ports that support 40-GigabitEthernet connectivity, OR 16 ports that support 100-GigabitEthernet connectivity; two power supply slots.
C9500-32QC-A	Network Advantage	
C9500-48Y4C-E	Network Essentials	48 SFP28 ports that support 1/10/25-GigabitEthernet connectivity; four QSFP uplink ports that supports up to 100/40-GigabitEthernet connectivity; two power supply slots.
C9500-48Y4C-A	Network Advantage	

Network Modules

The following table lists optional network modules for uplink ports available with some configurations .

Network Module	Description
C9500-NM-8X	Cisco Catalyst 9500 Series Network Module 8-port 1/10 Gigabit Ethernet with SFP/SFP+ Note the supported switch models (Base PIDs): • C9500-40X • C9500-16X

Network Module	Description
C9500-NM-2Q	Cisco Catalyst 9500 Series Network Module 2-port 40 Gigabit Ethernet with QSFP+ Note the supported switch models (Base PIDs): • C9500-40X • C9500-16X

Optics Modules

Cisco Catalyst Series Switches support a wide range of optics and the list of supported optics is updated on a regular basis. Use the Transceiver Module Group (TMG) Compatibility Matrix tool, or consult the tables at this URL for the latest transceiver module compatibility information: https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Compatibility Matrix

The following table provides software compatibility information between Cisco Catalyst 9500 Series Switches, Cisco Identity Services Engine, Cisco Access Control Server, and Cisco Prime Infrastructure.

Catalyst 9500, 9500-High Performance and 9500X	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
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**.

Catalyst 9500, 9500-High Performance and 9500X	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Fuji 16.9.6	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.5	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.4	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.3	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.2	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.1	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
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**.

Catalyst 9500, 9500-High Performance and 9500X	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
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[1]	512 MB[2]	256	1280 x 800 or higher	Small

1 We recommend 1 GHz
2 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)

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 Gibraltar 16.11.1	CAT9K_IOSXE	cat9k_iosxe.16.11.01.SPA.
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.11.01.S

Automatic Boot Loader Upgrade

When you upgrade from the existing release on your switch to a later or newer release for the first time, the boot loader may be automatically upgraded, based on the hardware version of the switch. If the boot loader is automatically upgraded, it will take effect on the next reload. If you go back to the older release after this, the boot loader is not downgraded. The updated boot loader supports all previous releases.

For subsequent Cisco IOS XE Everest 16.x.x, or Cisco IOS XE Fuji 16.x.x releases, if there is a new bootloader in that release, it may be automatically upgraded based on the hardware version of the switch when you boot up your switch with the new image for the first time.



Caution Do not power cycle your switch during the upgrade.

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE Gibraltar 16.11.1 first time	On Cisco Catalyst 9500 Series Switches, the boot loader may be upgraded to version 16.10.1r [FC1]. For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 16.10.1r[FC1], RELEASE SOFTWARE (P)`
	On Cisco Catalyst 9500 Series Switches - High Performance, the boot loader may be upgraded to version 16.11.1r[FC2]. For example:
	`System Bootstrap, Version 16.11.1r[FC2], RELEASE SOFTWARE (P)`
	`Compiled 03-01-2019 12:33:31.95 by rel`
	When using **install** commands to upgrade software, you may see this during the install operation:
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Wed Mar 06 18:03:28 Universal 2019 PLEASE DO NOT POWER CYCLE`
	`### BOOT LOADER UPGRADING`
	`waiting for upgrades to complete...`

Software Installation Commands

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

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

Summary of request platform software Commands **Note** **This table of commands is not supported on Cisco Catalyst 9500 Series Switches - High Performance.**	
`Device# request platform software package ?`	
clean	Cleans unnecessary package files from media
copy	Copies package to media
describe	Describes package content
expand	Expands all-in-one package to media
install	Installs the package
uninstall	Uninstalls the package
verify	Verifies In Service Software Upgrade (ISSU) software package compatibility

Changing the Default Interface and Upgrading or Downgrading in Install Mode (for Cisco Catalyst 9500 Series Switches - High Performance Only)

Before you begin

Read the entire section including the steps and only then proceed with performing the task.

Applicable Devices and Releases

This task is applicable to the following devices and releases:

When upgrading these devices ...	From...	To...
High Performance models of the Cisco Catalyst 9500 Series Switches (C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C. This includes standalone switches and switches where Cisco StackWise Virtual is configured.	An earlier Cisco IOS XE 16.x.x	Cisco IOS XE Gibraltar 16.11.1,

When downgrading these devices ...	From...	To...
High Performance models of the Cisco Catalyst 9500 Series Switches (C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C). This includes standalone switches and switches where Cisco StackWise Virtual is configured.	Cisco IOS XE Gibraltar 16.11.1	An earlier Cisco IOS XE 16.x.x

High Performance models were introduced in Cisco IOS XE Fuji 16.8.1a

Purpose

Starting in Cisco IOS XE Gibraltar 16.11.1, the above mentioned devices will bootup with interfaces in the default Layer 2 state. In all earlier releases, the default is Layer 3. This task describes what you have to do, to ensure that this change does not erase existing interface configuration or cause a network downtime, and how you can safely upgrade to or downgrade from Cisco IOS XE Gibraltar 16.11.1.



Note For all other Cisco Catalyst 9000 Series Switches, the default interface continues to be Layer 2.

Description

This task updates running configuration as follows:

- The **switchport** command is added to all Layer 2 interfaces.
- The **no switchport** command is added to all Layer 3 interfaces.

Applicable interfaces include physical ports, breakout interfaces, and port channels. It is not applicable to tunnels, SVIs, or sub-interfaces.



Note Any existing interface configuration is preserved.

Reason for this Change

The default interface is changed to Layer 2, to enable day 0 discovery when using Cisco Digital Network Architecture (DNA) Center (or Cisco DNA Center).

Interactions with other Features

None.

In Service Software Upgrade (ISSU) is not supported when you upgrade from an earlier Cisco IOS XE 16.x.x release to Cisco IOS XE Gibraltar 16.11.1, or when you downgrade from Cisco IOS XE Gibraltar 16.11.1 to an earlier Cisco IOS XE 16.x.x.

Available Methods

- You can use a script that automatically makes the necessary running configuration changes and then upgrade or downgrade. This document covers only this method.
- You can manually update running configuration for all interfaces and then upgrade or downgrade.

Procedure

Step 1 Backup the current running configuration.

```
Switch# copy running-config flash:backup-config
```

Step 2 Disable the auto-archive feature, and any similar scripts.

```
Switch# configure terminal
Switch(config)# no archive
```

You can re-enable these features after completing this task.

Step 3 Executing the script (in a later step) will generate two new files in flash (currentconfig.txt & newconfig.txt), ensure that you do not have files with the same file names in flash, else they will be overwritten.

Step 4 Copy the new image, set the boot variable, and save configuration.

a) Copy the new image.

- For standalone switches: Copy the new image to bootflash. The example below uses TFTP to download to bootflash:

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.11.01.SPA.bin flash:

Destination filename [cat9k_iosxe.16.11.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.11.01.SPA.bin...
Loading /cat9k_iosxe.16.11.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]

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

- For switches where Cisco StackWise Virtual is configured: Copy the new image to bootflash and standby bootflash. The example below uses TFTP to download to bootflash and standby bootflash:

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.11.01.SPA.bin flash:
<output truncated>
### and
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.11.01.SPA.bin stby-bootflash:
<output truncated>
```

b) Set the boot variable.

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

c) Save boot settings.

```
Switch# write memory
```

Step 5 Copy the script, save it as a text file, and copy it to bootflash.

a) Save the script as a text file called **defaultPortUpdate.tcl**.

```
###Start of the script defaultPortUpdate.tcl
set currentconfig ""
set newconfig ""
set currentconfig "sh running-config"
set currentconfig [exec $currentconfig]

puts "Taking backup of current running config ....\n"
###copying current running config to flash:currentconfig.txt
set fp [open "currentconfig.txt" w+]
puts $fp $currentconfig
close $fp
puts "################################################################"
puts "Current running config is stored in flash:currentconfig.txt "
puts "################################################################"

###read from flash:currentconfig.txt
set fp [open "currentconfig.txt" r]
set currentconfig_1 [read $fp]
close $fp
```

```
puts "\nPreparing for the new configuration for port mode defaults"
puts "\nNew modified configuration file will have \"switchport\" for L2 and \"no
switchport\" for L3 on physical interfaces and port channels\n"
####look for "interface name " with "no ip address", "ip address" and udpdate as
"interface name" \n "no switchport" \n "ip address"/"no ip address"
set intflist "sh ip interface brief"
set intflist [exec $intflist]

foreach line1 [split $intflist "\n"] {
    if [regexp "TwentyFiveGigE\[1-6\]/0/(\[1-9\]|\[1-9\]\[0-9\])" $line1 match3] {
        lappend intflist1 $match3
    } elseif {[regexp "FortyGigabitEthernet\[1-6\]/0/(\[1-9\]|\[1-9\]\[0-9\])" $line1
match4] || [regexp "Fo(\[1-6\]/0/(\[1-9\]|\[1-9\]\[0-9\]))" $line1 match4 m1]} {
        regsub "Fo$m1" $match4 "FortyGigabitEthernet$m1" match4
        lappend intflist1 $match4
    } elseif {[regexp "HundredGigE\[1-6\]/0/(\[1-9\]|\[1-9\]\[0-9\])" $line1 match5] &&
 ![regexp "HundredGigE\[1-6\]/0/(\[1-9\]|\[1-9\]\[0-9\])/" $line1 match5] } {
        lappend intflist1 $match5
    } elseif [regexp "HundredGigE\[1-6\]/0/(\[1-9\]|\[1-9\]\[0-9\])/\[1-4\]" $line1
match6] {
        lappend intflist1 $match6
   } elseif [regexp "Port-channel(\[1-9\]|\[1-9\]\[0-9\]|\[1-9\]\[0-9\]\[0-9\])" $line1
 match7] {
        lappend intflist1 $match7
    }
}

set newconfig $currentconfig_1
foreach interface $intflist1 {
    set match1 "sh run interface $interface"
    set match1 [exec $match1]
    if {![regexp "stackwise-virtual" $match1]} {
        if {[regexp "ip address" $match1] } {
           #puts "hhhi $interface bbby"
            regsub "interface $interface" $newconfig  "interface $interface\n no
switchport" newconfig
        }
        if {![regexp "ip address" $match1 ]} {
           #puts "hhhi $interface bbby"
          regsub "interface $interface" $newconfig  "interface $interface\n switchport"
 newconfig
        }
    }
}

puts "################################################################"
puts "New modified configuration file is stored at flash:newconfig.txt, kindly keep this
 file stored as a backup for future use"
puts "################################################################"

###udpated new config is present in flash:newconfig.txt
set fd [open "newconfig.txt" w+]
puts $fd $newconfig
close $fd
set fd [open "newconfig_backup.txt" w+]
puts $fd $newconfig
close $fd

puts "!!! Script exeuction Done !!!"
```

###End of script defaultPortUpdate.tcl

b) Copy the script to bootflash. The example below uses TFTP to download to bootflash.

```
Switch# copy tftp://10.8.0.6//defaultPortUpdate.tcl bootflash:
Destination filename [defaultPortUpdate.tcl]?
Accessing tftp://10.8.0.6//defaultPortUpdate.tcl...
Loading /defaultPortUpdate.tcl from 10.8.0.6 (via GigabitEthernet0/0):
!
3130 bytes copied in 0.038 secs (82368 bytes/sec)
```

c) Verify that the script has been copied to bootflash.

```
Switch# dir bootflash:defaultPortUpdate.tcl

Directory of bootflash:/defaultPortUpdate.tcl
243483  -rw-            3130  Mar 30 2019 12:51:47 +05:30  defaultPortUpdate.tcl
11250098176 bytes total (4172689408 bytes free)
```

Step 6 Run the script.

```
Switch# tclsh flash:defaultPortUpdate.tcl
Taking backup of current running config ....

##############################################################
Current running config is stored in flash:currentconfig.txt
##############################################################

Preparing for the new configuration for port mode defaults

New modified configuration file will have "switchport" for L2 and "no switchport" for L3
on physical interfaces and port channels

##############################################################
New modified configuration file is stored at flash:newconfig.txt, kindly keep this file
stored as a backup for future use
##############################################################

ATTENTION: kindly configure boot file as flash:newconfig.txt to boot with modified
configuration on your next reload

!!! Script exeuction Done !!!
```

Step 7 Verify that two new `.txt` files are saved in bootflash.

```
Switch# dir bootflash:newconfig.txt
Directory of bootflash:/newconfig.txt
243485  -rw-            13126  Mar 30 2019 12:53:08 +05:30  newconfig.txt
11250098176 bytes total (4172656640 bytes free)

Switch# dir bootflash:currentconfig.txt
Directory of bootflash:/currentconfig.txt
243484  -rw-            13151  Mar 30 2019 12:53:08 +05:30  currentconfig.txt
11250098176 bytes total (4172656640 bytes free)
```

Step 8 Copy file `newconfig.txt` to startup configuration.

Important
Do NOT **write memory**or **save running-startup**.

- For standalone switches: Copy the file to startup configuration.

```
Switch# copy flash:newconfig.txt nvram:startup-config
```

- For switches where Cisco StackWise Virtual is configured: Copy the file to startup configuration of the active and standby switches.

```
Switch# copy flash:newconfig.txt nvram:startup-config
and
Switch# copy flash:newconfig.txt stby-nvram:startup-config
```

Step 9 Install the new image to flash.

```
Switch# install add file flash:cat9k_iosxe.16.11.01.SPA.bin activate commit
install_add_activate_commit: START Wed Mar 06 19:54:51 UTC 2019

%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.11.01.SPA.bininstall_add_activate_commit: Adding PACKAGE

This operation requires a reload of the system. Do you want to proceed?
Please confirm you have changed boot config to flash:packages.conf [y/n]y
<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 10 Check the flash partition

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

```
Switch# dir flash:*.pkg

Switch# dir flash:*.conf
```

Step 11 Check the software version

The sample output below shows that the Cisco IOS XE Gibraltar 16.11.1 version is successfully installed on the switch.

```
Switch# show version
Cisco IOS XE Software, Version 16.11.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.11.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
<output truncated>
```

Step 12 Check configuration updates.

Executing the script ensures that there is no functional impact or change in behavior after upgrading to Cisco IOS XE Gibraltar 16.11.1. If there were configured interfaces before upgrade, after upgrade, the old configuration is preserved - as displayed in the examples below:

```
Switch# show running-config
```

Before Upgrade	After Upgrade

interface HundredGigE1/0/31
    no ip address
!
	interface HundredGigE1/0/31
	    no switchport
	    no ip address
	!

Before Upgrade	After Upgrade

`interface HundredGigE1/0/32`
`  ip address 11.12.1.1 255.255.255.0`
`!`
	`interface HundredGigE1/0/32`
	`  no switchport`
	`  ip address 11.12.1.1 255.255.255.0`
	`!`

`interface HundredGigE1/0/28`
`  switchport`
`  switchport access vlan 54`
`  switchport mode access`
`!`
	`interface HundredGigE1/0/28`
	`  switchport`
	`  switchport access vlan 54`
	`  switchport mode access`
	`!`

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 Gibraltar 16.11.x
Cisco IOS XE Everest 16.6.2 and later	On Cisco Catalyst 9500 Series Switches either **install** commands or **request platform software** commands	

Warning Do not use this procedure to upgrade any of the High Performance models to Cisco IOS XE Gibraltar 16.11.1. Doing so will erase certain configuration. For these models, follow the procedure described here:Changing the Default Interface and Upgrading or Downgrading in Install Mode (for Cisco Catalyst 9500 Series Switches - High Performance Only) , on page 21

The sample output in this section displays upgrade from

- Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.11.1 using **request platform software** commands.
- Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.11.1 using **install** commands.

Procedure

Step 1 Clean Up

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

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

The following sample output displays the cleaning up of unused files, by using the **request platform software package clean** command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.11.1.

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

The following files will be deleted:
[1]:
/flash/cat9k-cc_srdriver.16.06.01..SPA.pkg
/flash/cat9k-espbase.16.06.01.SPA.pkg
/flash/cat9k-guestshell.16.06.01.SPA.pkg
/flash/cat9k-rpbase.16.06.01.SPA.pkg
/flash/cat9k-rpboot.16.06.01.SPA.pkg
/flash/cat9k-sipbase.16.06.01.SPA.pkg
/flash/cat9k-sipspa.16.06.01.SPA.pkg
/flash/cat9k-srdriver.16.06.01.SPA.pkg
/flash/cat9k-webui.16.06.01.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/cat9k_iosxe.16.06.01.SPA.bin
/flash/packages.conf.00-
```

```
Do you want to proceed? [y/n]y
[1]:
Deleting file flash:cat9k-cc_srdriver.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:cat9k_iosxe.16.06.01.SPA.bin ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
Switch#
```

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command, for upgrade scenario Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.11.1:

```
Switch# install remove inactive

install_remove: START Wed Mar 06 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.16.06.03.SPA.pkg
/flash/cat9k-espbase.16.06.03.SPA.pkg
/flash/cat9k-guestshell.16.06.03.SPA.pkg
/flash/cat9k-rpbase.16.06.03.SPA.pkg
/flash/cat9k-rpboot.16.06.03.SPA.pkg
/flash/cat9k-sipbase.16.06.03.SPA.pkg
/flash/cat9k-sipspa.16.06.03.SPA.pkg
/flash/cat9k-srdriver.16.06.03.SPA.pkg
/flash/cat9k-webui.16.06.03.SPA.pkg
/flash/cat9k-wlc.16.06.03.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.06.03.SPA.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
[1] Post_Remove_Cleanup package(s) on switch 1
[1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup
```

```
SUCCESS: install_remove Wed Mar 06 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.11.01.SPA.bin flash:

Destination filename [cat9k_iosxe.16.11.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.11.01.SPA.bin...
Loading /cat9k_iosxe.16.11.01.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 Mar 06 2019 10:18:11 -07:00 cat9k_iosxe.16.11.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

Step 3 Set boot variable

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

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

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

b) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

c) **show boot system**

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

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

```
Switch# show boot system
```

Step 4 Software install image to flash

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

The following sample output displays installation of the Cisco IOS XE Gibraltar 16.11.1 software image to flash, by using the **request platform software package install** command, for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.11.1.

```
Switch# request platform software package install switch all file
flash:cat9k_iosxe.16.11.01.SPA.bin

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

Expanding image file: flash:cat9k_iosxe.16.11.01.SPA.bin
[]: Finished copying to switch
[1]: Expanding file
[1]: Finished expanding all-in-one software package in switch 1
SUCCESS: Finished expanding all-in-one software package.
[1]: Performing install
SUCCESS: install finished
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
Removed cat9k-sipbase.16.05.01a.SPA.pkg
Removed cat9k-sipspa.16.05.01a.SPA.pkg
Removed cat9k-srdriver.16.05.01a.SPA.pkg
Removed cat9k-webui.16.05.01a.SPA.pkg
Removed cat9k-wlc.16.05.01a.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.11.01.SPA.pkg
Added cat9k-espbase.16.11.01.SPA.pkg
Added cat9k-guestshell.16.11.01.SPA.pkg
Added cat9k-rpbase.16.11.01.SPA.pkg
Added cat9k-rpboot.16.11.01.SPA.pkg
Added cat9k-sipbase.16.11.01.SPA.pkg
Added cat9k-sipspa.16.11.01.SPA.pkg
Added cat9k-srdriver.16.11.01.SPA.pkg
Added cat9k-webui.16.11.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[1]: Finished install successful on switch 1
Checking status of install on [1]
[1]: Finished install in switch 1
SUCCESS: Finished install: Success on [1]
```

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

The following sample output displays installation of the Cisco IOS XE Gibraltar 16.11.1 software image to flash, by using the **install add file activate commit** command, for upgrade scenario Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.11.1:

```
Switch# install add file flash:cat9k_iosxe.16.11.01.SPA.bin activate commit

install_add_activate_commit: START Wed Mar 06 19:54:51 UTC 2019

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

```
 configuration...

[OK]Modified configuration has been saved

*Mar 06 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 06 19:54:55 install_engine.sh:

%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.11.01.SPA.bininstall_add_activate_commit: Adding PACKAGE

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

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.11.01.SPA.bin to the selected switch(es)
Finished initial file syncing

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

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.16.11.01.SPA.pkg
/flash/cat9k-webui.16.11.01.SPA.pkg
/flash/cat9k-srdriver.16.11.01.SPA.pkg
/flash/cat9k-sipspa.16.11.01.SPA.pkg
/flash/cat9k-sipbase.16.11.01.SPA.pkg
/flash/cat9k-rpboot.16.11.01.SPA.pkg
/flash/cat9k-rpbase.16.11.01.SPA.pkg
/flash/cat9k-guestshell.16.11.01.SPA.pkg
/flash/cat9k-espbase.16.11.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.11.01.SPA.pkg

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

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

*Mar 06 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 06 19:57:41 rollback_timer.sh:

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

Install will reload the system now!
SUCCESS: install_add_activate_commit Wed Mar 06 19:57:48 UTC 2019
Switch#
```

Note

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

Step 5 **dir flash:**

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

The following is sample output of the **dir flash:** command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.11.1:

```
Switch# dir flash:*.pkg

Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104   Jul 26 2017 09:52:41 -07:00 cat9k-cc_srdriver.16.05.01a.SPA.pkg
475141 -rw- 70333380  Jul 26 2017 09:52:44 -07:00 cat9k-espbase.16.05.01a.SPA.pkg
475142 -rw- 13256     Jul 26 2017 09:52:44 -07:00 cat9k-guestshell.16.05.01a.SPA.pkg
475143 -rw- 349635524 Jul 26 2017 09:52:54 -07:00 cat9k-rpbase.16.05.01a.SPA.pkg
475149 -rw- 24248187  Jul 26 2017 09:53:02 -07:00 cat9k-rpboot.16.05.01a.SPA.pkg
475144 -rw- 25285572  Jul 26 2017 09:52:55 -07:00 cat9k-sipbase.16.05.01a.SPA.pkg
475145 -rw- 20947908  Jul 26 2017 09:52:55 -07:00 cat9k-sipspa.16.05.01a.SPA.pkg
475146 -rw- 2962372   Jul 26 2017 09:52:56 -07:00 cat9k-srdriver.16.05.01a.SPA.pkg
475147 -rw- 13284288  Jul 26 2017 09:52:56 -07:00 cat9k-webui.16.05.01a.SPA.pkg
475148 -rw- 13248     Jul 26 2017 09:52:56 -07:00 cat9k-wlc.16.05.01a.SPA.pkg

491524 -rw- 25711568  Mar 06 2019 11:49:33 -07:00 cat9k-cc_srdriver.16.11.01.SPA.pkg
491525 -rw- 78484428  Mar 06 2019 11:49:35 -07:00 cat9k-espbase.16.11.01.SPA.pkg
491526 -rw- 1598412   Mar 06 2019 11:49:35 -07:00 cat9k-guestshell.16.11.01.SPA.pkg
491527 -rw- 404153288 Mar 06 2019 11:49:47 -07:00 cat9k-rpbase.16.11.01.SPA.pkg
491533 -rw- 31657374  Mar 06 2019 11:50:09 -07:00 cat9k-rpboot.16.11.01.SPA.pkg
491528 -rw- 27681740  Mar 06 2019 11:49:48 -07:00 cat9k-sipbase.16.11.01.SPA.pkg
491529 -rw- 52224968  Mar 06 2019 11:49:49 -07:00 cat9k-sipspa.16.11.01.SPA.pkg
491530 -rw- 31130572  Mar 06 2019 11:49:50 -07:00 cat9k-srdriver.16.11.01.SPA.pkg
491531 -rw- 14783432  Mar 06 2019 11:49:51 -07:00 cat9k-webui.16.11.01.SPA.pkg
491532 -rw- 9160      Mar 06 2019 11:49:51 -07:00 cat9k-wlc.16.11.01.SPA.pkg

11353194496 bytes total (8963174400 bytes free)
```

The following is sample output of the **dir flash:** command for the Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.11.1 upgrade scenario:

```
Switch# dir flash:

Directory of flash:/
475140 -rw- 2012104   Jul 26 2017 09:52:41 -07:00 cat9k-cc_srdriver.16.06.03.SPA.pkg
475141 -rw- 70333380  Jul 26 2017 09:52:44 -07:00 cat9k-espbase.16.06.03.SPA.pkg
475142 -rw- 13256     Jul 26 2017 09:52:44 -07:00 cat9k-guestshell.16.06.03.SPA.pkg
475143 -rw- 349635524 Jul 26 2017 09:52:54 -07:00 cat9k-rpbase.16.06.03.SPA.pkg
475149 -rw- 24248187  Jul 26 2017 09:53:02 -07:00 cat9k-rpboot.16.06.03.SPA.pkg
475144 -rw- 25285572  Jul 26 2017 09:52:55 -07:00 cat9k-sipbase.16.06.03.SPA.pkg
475145 -rw- 20947908  Jul 26 2017 09:52:55 -07:00 cat9k-sipspa.16.06.03.SPA.pkg
475146 -rw- 2962372   Jul 26 2017 09:52:56 -07:00 cat9k-srdriver.16.06.03.SPA.pkg
475147 -rw- 13284288  Jul 26 2017 09:52:56 -07:00 cat9k-webui.16.06.03.SPA.pkg
475148 -rw- 13248     Jul 26 2017 09:52:56 -07:00 cat9k-wlc.16.06.03.SPA.pkg

491524 -rw- 25711568  Mar 06 2019 11:49:33 -07:00 cat9k-cc_srdriver.16.11.01.SPA.pkg
491525 -rw- 78484428  Mar 06 2019 11:49:35 -07:00 cat9k-espbase.16.11.01.SPA.pkg
491526 -rw- 1598412   Mar 06 2019 11:49:35 -07:00 cat9k-guestshell.16.11.01.SPA.pkg
491527 -rw- 404153288 Mar 06 2019 11:49:47 -07:00 cat9k-rpbase.16.11.01.SPA.pkg
491533 -rw- 31657374  Mar 06 2019 11:50:09 -07:00 cat9k-rpboot.16.11.01.SPA.pkg
491528 -rw- 27681740  Mar 06 2019 11:49:48 -07:00 cat9k-sipbase.16.11.01.SPA.pkg
```

```
491529 -rw- 52224968  Mar 06 2019 11:49:49 -07:00 cat9k-sipspa.16.11.01.SPA.pkg
491530 -rw- 31130572  Mar 06 2019 11:49:50 -07:00 cat9k-srdriver.16.11.01.SPA.pkg
491531 -rw- 14783432  Mar 06 2019 11:49:51 -07:00 cat9k-webui.16.11.01.SPA.pkg
491532 -rw- 9160      Mar 06 2019 11:49:51 -07:00 cat9k-wlc.16.11.01.SPA.pkg

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

The following sample output displays the .conf files in the flash partition; note the three .conf files:

- `packages.conf`—the file that has been re-written with the newly installed .pkg files
- `cat9k_iosxe.16.11.01.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 Mar 06 2019 10:59:16 -07:00 packages.conf
516098 -rw- 7406 Mar 06 2019 10:58:08 -07:00 cat9k_iosxe.16.11.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

Step 6 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

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

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

c) **show version**

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

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

The following sample output of the **show version** command displays the Cisco IOS XE Gibraltar 16.11.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.11.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.11.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 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 via " 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 Gibraltar 16.11.x	On Cisco Catalyst 9500 Series Switches, either **install** commands or **request platform software** commands	Cisco IOS XE Gibraltar 16.10.x or an earlier release.

Warning Do not use this procedure to downgrade any of the High Performance models from Cisco IOS XE Gibraltar 16.11.1 to any earlier release. Doing so will erase certain configuration. For these models, follow the procedure described here:Changing the Default Interface and Upgrading or Downgrading in Install Mode (for Cisco Catalyst 9500 Series Switches - High Performance Only) , on page 21

The sample output in this section shows downgrade from Cisco IOS XE Gibraltar 16.11.1 to Cisco IOS XE Everest 16.6.1, by using the **install** commands.

Important 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.

Procedure

Step 1 Clean Up

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

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

The following sample output displays the cleaning up of Cisco IOS XE Gibraltar 16.11.1 files using the **install remove inactive** command:

```
Switch# install remove inactive

install_remove: START Wed Mar 06 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:
```

```
/flash/cat9k-cc_srdriver.16.11.01.SPA.pkg
/flash/cat9k-espbase.16.11.01.SPA.pkg
/flash/cat9k-guestshell.16.11.01.SPA.pkg
/flash/cat9k-rpbase.16.11.01.SPA.pkg
/flash/cat9k-rpboot.16.11.01.SPA.pkg
/flash/cat9k-sipbase.16.11.01.SPA.pkg
/flash/cat9k-sipspa.16.11.01.SPA.pkg
/flash/cat9k-srdriver.16.11.01.SPA.pkg
/flash/cat9k-webui.16.11.01.SPA.pkg
/flash/cat9k-wlc.16.11.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.11.01.SPA.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
[1] Post_Remove_Cleanup package(s) on switch 1
[1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Wed Mar 06 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.06.01.SPA.bin flash:

Destination filename [cat9k_iosxe.16.06.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.06.01.SPA.bin...
Loading /cat9k_iosxe.16.06.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 508584771 bytes]
508584771 bytes copied in 101.005 secs (5035244 bytes/sec)
```

b) **dir flash:**

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

```
Switch# dir flash:*.bin
Directory of flash:/*.bin

Directory of flash:/

434184 -rw- 508584771 Mar 06 2019 13:35:16 -07:00 cat9k_iosxe.16.06.01.SPA.bin
```

```
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Downgrade software image

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

The following example displays the installation of the Cisco IOS XE Everest 16.6.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.16.06.01.SPA.bin activate commit

install_add_activate_commit: START Wed Mar 06 19:54:51 UTC 2019

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

[OK]Modified configuration has been saved

*Mar 06 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 06 19:54:55 install_engine.sh:
 %INSTALL-
5-INSTALL_START_INFO: Started install one-shot flash:cat9k_iosxe.16.06.01.SPA.bin
install_add_activate_commit: Adding PACKAGE

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

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.06.01.SPA.bin to the selected switch(es)
Finished initial file syncing

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

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.16.06.01.SPA.pkg
/flash/cat9k-webui.16.06.01.SPA.pkg
/flash/cat9k-srdriver.16.06.01.SPA.pkg
/flash/cat9k-sipspa.16.06.01.SPA.pkg
/flash/cat9k-sipbase.16.06.01.SPA.pkg
/flash/cat9k-rpboot.16.06.01.SPA.pkg
/flash/cat9k-rpbase.16.06.01.SPA.pkg
/flash/cat9k-guestshell.16.06.01.SPA.pkg
/flash/cat9k-espbase.16.06.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.06.01.SPA.pkg

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

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

*Mar 06 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 06 19:57:41 rollback_timer.sh:
 %INSTALL-
5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Install auto abort timer will expire in 7200 seconds
[1] Commit package(s) on switch 1
[1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit Wed Mar 06 19:57:48 UTC 2019
Switch#
```

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

Step 4 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

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

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

Note
When you downgrade the software image, the boot loader does not automatically downgrade. It remains updated.

c) **show version**

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

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

The following sample output of the **show version** command displays the Cisco IOS XE Everest 16.6.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.06.01
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
```

```
Compiled Fri 16-Mar-18 06:38 by mcpre
<output truncated>
```

Licensing

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

License Levels

The software features available on Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance fall under these base or add-on license levels.

Base Licenses

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

Add-On Licenses

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

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

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

License Types

The following license types are available:

- Permanent—for a license level, and without an expiration date.
- Term—for a license level, and for a three, five, or seven year period.
- Evaluation—a license that is not registered.

License Levels - Usage Guidelines

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

- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- When ordering an add-on license with a base license, note the combinations that are permitted and those that are not permitted:

Table 3: Permitted Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No
Network Advantage	Yes[3]	Yes

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

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

Cisco Smart Licensing

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

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- Unified Management: Cisco License Central provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco License Central. For a more detailed overview on Cisco Licensing, visit the Licensing Hub.



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

Deploying Smart Licensing

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

Procedure

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

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

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

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

Step 3 Complete the Cisco Smart Software Manager set up.

a) Accept the Smart Software Licensing Agreement.

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

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

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

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

With this,

- The device is now in an authorized state and ready to use.
- The licenses that you have purchased are displayed in your Smart Account.

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

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

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

How Upgrading or Downgrading Software Affects Smart Licensing

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



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

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

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

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

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

Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst 9500 Series Switches datasheet at:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/datasheet-c78-738978.html

Limitations and Restrictions

With Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance—If a feature is not supported on a switch model, you do not have to factor in any limitations or restrictons that may be listed here. If limitations or restrictions are listed for a feature that is supported, check if model numbers are specified, to know if they apply. If model numbers are not specified, the limitations or restrictons apply to all models in the series.

- Auto negotiation

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

  Auto negotiation is always ON for GLC-T and GLC-TE and cannot be disabled. This is applicable to GLC-T and GLC-TE on C9500-48Y4C and C9500-24Y4C models of the series.

- Cisco StackWise Virtual
  - On Cisco Catalyst 9500 Series Switches, when Cisco StackWise Virtual is configured, breakout ports using 4X10G breakout cables, or the Cisco Cisco QSFP to SFP or SFP+ Adapter (QSA) module can only be used as data ports; they cannot be used to configure StackWise Virtual links (SVLs) or dual-active detective (DAD) links.
  - On Cisco Catalyst 9500 Series Switches - High Performance, when Cisco StackWise Virtual is configured, breakout ports using 4X25G and 4X10G breakout cables, or the Cisco QSA module can only be used as data ports; they cannot be used to configure SVLs or DAD links.

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

- 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.

- 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 switched virtual interfaces (SVIs), port-channel, loopback, tunnels.
  - You can not configure multiple flow monitors of same type (ipv4, ipv6 or datalink) on the same interface for same direction.

- Hardware limitations:
  - Use the MODE button to switch-off the beacon LED.
  - All port LED behavior is undefined until interfaces are fully initialized.
  - 1G with Cisco QSA Module (CVR-QSFP-SFP10G) is not supported on the uplink ports of the C9500-24Y4C and C9500-48Y4C models.
  - The following limitations apply to Cisco QSA Module (CVR-QSFP-SFP10G) when Cisco 1000Base-T Copper SFP (GLC-T) or Cisco 1G Fiber SFP Module for Multimode Fiber are plugged into the QSA module:
    - 1G Fiber modules over QSA do not support autonegotiation. Auto-negotiation should be disabled on the far-end devices.
    - Although visible in the CLI, the command [**no**] **speed nonegotiate** is not supported with 1G Fiber modules over QSA.
    - Only GLC-T over QSA supports auto-negotiation.
    - GLC-T supports only port speed of 1000 Mb/s over QSA. Port speeds of 10/100-Mb/s are not supported due to hardware limitation.
  - When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, autonegotiation is enabled by default. If the other end of the line does not support autonegotation, the link does not come up.
  - Autonegotiation is not supported on HundredGigabitEthernet1/0/49 to HundredGigabitEthernet1/0/52 uplink ports of the C9500-48Y4C models, and HundredGigabitEthernet1/0/25 to HundredGigabitEthernet1/0/28 uplink ports of the C9500-24Y4C models. Disable autonegotiation on the peer device if you are using QSFP-H40G-CUxx and QSFP-H40G-ACUxx cables.
  - For QSFP-H100G-CUxx cables, the C9500-48Y4C and C9500-24Y4C models support the cables only if both sides of the connection are either C9500-48Y4C or C9500-24Y4C.

- Interoperability limitations—When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, if one end of the 40G link is a Catalyst 9400 Series Switch and the other end is a Catalyst 9500 Series Switch, the link does not come up, or comes up on one side and stays down on the other. To avoid this interoperability issue between devices, apply the the **speed nonegotiate** command on the Catalyst 9500 Series Switch interface. This command disables autonegotiation and brings the link up. To restore autonegotiation, use the **no speed nonegotiation** command.

- In-Service Software Upgrade (ISSU)—On Cisco Catalyst 9500 Series Switches (C9500-12Q, C9500-16X, C9500-24Q, C9500-40X), ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.10.x or to Cisco IOS XE Gibraltar 16.11.x is not supported.

- 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.

- 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.

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

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

- VLAN Restriction—It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.
- Wired Application Visibility and Control limitations:
  - NBAR2 (QoS and Protocol-discovery) configuration is allowed only on wired physical ports. It is not supported on virtual interfaces, for example, VLAN, port channel nor other logical interfaces.
  - NBAR2 based match criteria ‘match protocol’ is allowed only with marking or policing actions. NBAR2 match criteria will not be allowed in a policy that has queuing features configured.
  - ‘Match Protocol’: up to 256 concurrent different protocols in all policies.
  - NBAR2 and Legacy NetFlow cannot be configured together at the same time on the same interface. However, NBAR2 and wired AVC Flexible NetFlow can be configured together on the same interface.
  - Only IPv4 unicast (TCP/UDP) is supported.
  - AVC is not supported on management port (Gig 0/0)
  - NBAR2 attachment should be done only on physical access ports. Uplink can be attached as long as it is a single uplink and is not part of a port channel.
  - Performance—Each switch member is able to handle 500 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.

  - Scale—Able to handle up to 5000 bi-directional flows per 24 access ports and 10000 bi-directional flows per 48 access ports.

- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.
- Embedded Event Manager—Identity event detector is not supported on Embedded Event Manager.
- Secure Password Migration—Type 6 encrypted password is supported from Cisco IOS XE Gibraltar 16.10.1 and later releases. Autoconversion to password type 6 is supported from Cisco IOS XE Gibraltar 16.11.1 and later releases.

  If the startup configuration has a type 6 password and you downgrade to a version in which type 6 password is not supported, you can/may be locked out of the device.
- The File System Check (fsck) utility is not supported in install mode.
- Switch Web UI allows configuration of data VLANs only and not voice VLANs. If you remove a voice VLAN configured to an interface using the Web UI, then all data VLANs associated with the interface are also removed by default.

Caveats

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

Cisco Bug Search Tool

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

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

Open Caveats in Cisco IOS XE Gibraltar 16.11.x

Identifier	Applicable Models	Description
CSCvm65080	Catalyst 9500	usbflash1 entries are displayed multiple times in sh inventory o/p after multiple SSO
CSCvm86748	Catalyst 9500	9500-40x :phyloop back fails for forty gig ports

Resolved Caveats in Cisco IOS XE Gibraltar 16.11.1

Identifier	Applicable Models	Description
CSCvk00432	All models	Memory leak in alloc_repexp_entry caused by alloc_ril_index failure
CSCvm45417	All models	Cat9K HA/ 16.9.x,16.10.x- Connectivity issue due to wrong dest MAC rewrite for routed packet

Identifier	Applicable Models	Description
CSCvm94132	All models	AAL-INFRA:L2 failed to get ID handle
CSCvo19717	All models	crash in fib_path_list_walk_apply (cisco.comp/cfc_cefmpls/cef/src/fib_path_list_deps.c)
CSCvd54077	Catalyst 9500	c9500: Far-end 10GE ports flap up-down-up when Near end switch boots
CSCvi48988	Catalyst 9500	SNMP timeout when querying entSensorValueEntry
CSCvm69029	Catalyst 9500	Yang Get-config shows all the pwd configured on switch instead it should show only last updated pwd
CSCvm77197	Catalyst 9500	C9300 : %IOSXE-2-PLATFORM: Switch 1 R0/0: kernel: EXT2-fs (sda1): error:
CSCvm86478	Catalyst 9500	RMON statistics and RMON MIB absent in cat9K
CSCvn21168	Catalyst 9500	Configure for usb on the switch are gone after renumber the switch
CSCvo03530	Catalyst 9500	C9500- Remote side link stays up on reload with GLC-T/QSA.
CSCvo48808	Catalyst 9500	QSFP-40G-SR4 does not breakout in C9500-16X
CSCvj76260	Catalyst 9500 High Performance	C9500 SVL: Physical Interfaces Down on the Standby Switch
CSCvn17436	Catalyst 9500 High Performance	Memory leak in reflector.sh
CSCvn45646	Catalyst 9500 High Performance	Ports are getting into "INACTIVE state" on reload or sso on SF-SVL
CSCvn60882	Catalyst 9500 High Performance	CVR-QSFP-SFP10G V02 May get un-recognised or goes to error disabled state upon installation
CSCvn83359	Catalyst 9500 High Performance	IOSD Memory Leak in SVL
CSCvo21753	Catalyst 9500 High Performance	9500H/9600 SVL:MemLeak observed in chasync.sh
CSCvo25527	Catalyst 9500 High Performance	9500H SVL:When used 3rd party xcvrs intf not linking up and hence SVL come up as dual active

Troubleshooting

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

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

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

Related Documentation

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

All support documentation for Cisco Catalyst 9500 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/tsd-products-support-series-home.html

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

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: https://cfnng.cisco.com/mibs

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

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)

© 2019 Cisco Systems, Inc. All rights reserved.