Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Everest 16.6.x

First Published: July 31, 2017
Last Updated: September 30, 2019

This release note gives an overview of the hardware and software with the Cisco IOS XE Everest 16.6.x, on the Cisco Catalyst 9500 Series Switches.

Unless otherwise noted, the terms switch and device refer to a standalone switch.

• For information about unsupported features, see Important Notes, page 9
• For information about software and hardware restrictions and limitations, see Limitations and Restrictions, page 31.
• For information about open issues with the software, see Caveats, page 34.

Introduction

Cisco Catalyst 9500 Series Switches are Cisco's lead purpose-built fixed core and aggregation enterprise switching platform built for security, IoT and Cloud.

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

Cisco Catalyst 9500 Series Switches are purpose-built 40 Gigabit switches, targeted for enterprise campus, delivering unmatched table scales (MAC/route/ACL) and buffering for enterprise applications. It offers non-blocking 40G (QSFP) switches with granular port densities that fit diverse campus needs. The series also supports all the foundational high availability capabilities, and redundant platinum rated power supplies and fans.
Whats New in Cisco IOS XE Everest 16.6.7
There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.6
There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.5
There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.4a
There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.4
There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.3
There are no new hardware and software features in this release.
## Whats New in Cisco IOS XE Everest 16.6.2

### Software Features in Cisco IOS XE Everest 16.6.2

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Install</td>
<td>The Software Install feature facilitates moving from one version of the software to another version in install mode. See System Management -&gt; Performing Device Setup Configuration.</td>
</tr>
<tr>
<td>YANG Data Models</td>
<td>YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to <a href="https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1662">https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1662</a>. Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same github location highlights changes that have been made in the release. (Network Essentials)</td>
</tr>
</tbody>
</table>
Whats New in Cisco IOS XE Everest 16.6.1

Hardware Features in Cisco IOS XE Everest 16.6.1

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 40-Gigabit Ethernet QSFP and 10-Gigabit Ethernet SFP Switch Models | These Cisco Catalyst 9500 Series Switches are supported:  
  - C9500-12Q—12 40-Gigabit Ethernet QSFP ports and two power supply slots  
  - C9500-40X-2Q—40 10-Gigabit Ethernet SFP ports and a 2-Port 40-Gigabit Ethernet (QSFP) network module on uplink ports; and two power supply slots  
  - C9500-40X—40 10-Gigabit Ethernet SFP ports and two power supply slots; support for optional network modules on uplink ports—8-Port 10 Gigabit Ethernet (SFP) and 2-Port 40 Gigabit Ethernet (QSFP)  
  - C9500-48X—40 10-Gigabit Ethernet SFP ports and an 8-Port 10-Gigabit Ethernet (SFP) network module on uplink ports; and two power supply slots  
  See the Cisco Catalyst 9500 Series Switches Hardware Installation Guide. |
| Cisco QSFP to SFP or SFP+ Adapter (Cisco QSA Module) —CVR-QSFP-SFP10G | The Cisco Catalyst 9500 Series Switches support the Cisco QSA Module, which is a pluggable adapter that converts a QSFP port into an SFP+ port. You can connect only an SFP+ module.  
  See SFP and QSFP Module Ports. |

Software Features in Cisco IOS XE Everest 16.6.1

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description and License Level Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>New in Wired Switching</td>
<td></td>
</tr>
</tbody>
</table>
  Cisco Discovery Protocol Bypass | A backward compatible mode, equivalent to not having Cisco Discovery Protocol support. When the feature is enabled, Cisco Discovery Protocol packets are received and transmitted unchanged. Received packets are not processed. No packets are generated. In this mode, 'bump-in-the-wire' behavior is applied to Cisco Discovery Protocol packets.  
  (Network Essentials and Network Advantage) |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Nonstop Forwarding (NSF) Support for IPv6</strong></td>
<td>Cisco NSF is now supported for IPv6 traffic. Cisco NSF works with the Stateful switchover (SSO) feature to minimize the amount of time a network is unavailable to its users following a switchover. See High Availability -&gt; Configuring NSF with SSO. (Network Advantage)</td>
</tr>
</tbody>
</table>
| **Cisco StackWise Virtual**                | A network system virtualization technology that pairs two switches into one virtual switch to simplify operational efficiency with a single control and management plane. The feature supports:  
  - Minimum Latency Load Balancing—Here, in a Cisco StackWise Virtual setup, Multichassis EtherChannel forwards traffic over the local link, irrespective of the hash result.  
  - Dual-active-detection using ePAGP—Involves detection of a dual-active scenario using on Multichassis EtherChannel, between the switches in a Cisco StackWise Virtual setup.  
  Note: On the Cisco Catalyst 9500 Series Switches, this feature is supported only on the C9500-24Q switch model. See High Availability -> Configuring Cisco StackWise Virtual. (Network Advantage) |
<p>| <strong>High Availability—Graceful Insertion and Removal (GIR)</strong> | Uses a maintenance mode to isolate the switch from the network in order to perform debugging, or an upgrade. GIR is supported for Layer 2 interface shutdown and the Intermediate System to Intermediate System (IS-IS) routing protocol. When you place the switch in maintenance mode, supported protocols are isolated, and Layer 2 interfaces are shut down. When normal mode is restored, the supported protocols and ports are brought back up. See High Availability -&gt; Configuring Graceful Insertion and Removal (GIR). (Network Advantage) |
| <strong>Internet Group Management Protocol (IGMP) Explicit Tracking</strong> | Enables a multicast device to explicitly track the membership of all multicast hosts in a particular multiaccess network. The explicit tracking of hosts, groups, and channels enables the device to keep track of each individual host that is joined to a particular group or channel. See IP Multicast Routing -&gt; IGMP Explicit Tracking. (Network Essentials and Network Advantage) |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Multicast with Virtual Private Networks (VPN) Routing Forwarding Table (VRF-Lite)</td>
<td>Allows a service provider to support two or more VPNs with overlapping IP addresses using one interface. VRF-Lite uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. See IP Multicast Routing -&gt; Configuring VRF-lite.</td>
</tr>
</tbody>
</table>
| Locator ID Separator Protocol (LISP) Extranet Support and Source Group Access Control List (SGACL) Cell Statistics | • LISP Extranet Support—Refers to subscriber to provider communication across instance IDs in a LISP network. With LISP Extranet support, hosts in VRF “A”, for example, can access shared resources in VRF “B”.  
• SGACL Cell Statistics—An enhancement in the `show cts role-based counters ipv4` command, to display all SGACL enforcement statistics for IPv4, providing visibility at the cell level. See Campus Fabric. |

(Network Advantage)
<table>
<thead>
<tr>
<th>Multiprotocol Label Switching</th>
<th>The following MPLS features are introduced in this release:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ethernet over MPLS (EoMPLS)</td>
<td>• EoMPLS—One of the Any Transport over MPLS (AToM) transport types. EoMPLS provides a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core. It encapsulates Ethernet protocol data units (PDUs) inside MPLS packets and uses label stacking to forward them across the MPLS network.</td>
</tr>
<tr>
<td>• Virtual Private LAN Services (VPLS)</td>
<td>• VPLS—A class of VPN that supports the connection of multiple sites in a single bridged domain over a managed IP/MPLS network. VPLS uses the provider core to join multiple attachment circuits together, to simulate a virtual bridge that connects the multiple attachment circuits together.</td>
</tr>
<tr>
<td>• EIGRP MPLS VPN PE-CE Site of Origin (SoO)</td>
<td>• EIGRP MPLS VPN PE-CE 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 and is used to manage MPLS VPN traffic, and to prevent transient routing loops from occurring in complex and mixed network topologies.</td>
</tr>
<tr>
<td>• Route Target Rewrite</td>
<td>• Route Target Rewrite—Allows the replacement of route targets on incoming and outgoing Border Gateway Protocol (BGP) updates. Route targets are carried as extended community attributes in BGP Virtual Private Network IP Version 4 (VPNv4) updates. Route target extended community attributes are used to identify a set of sites and VPN routing and forwarding (VRF) instances that can receive routes with a configured route target.</td>
</tr>
<tr>
<td>• external BGP (eBGP) and internal BGP (iBGP) OR eiBGP</td>
<td>• eiBGP—Enables you to configure multipath load balancing with both eBGP and iBGP paths in Border Gateway Protocol (BGP) networks that are configured to use MPLS VPNs. The feature provides improved load balancing deployment and service offering capabilities and is useful for multi-homed autonomous systems and Provider Edge (PE) routers that import both eBGP and iBGP paths from multihomed and stub networks.</td>
</tr>
<tr>
<td>• IPv6 Provider Edge over MPLS (6PE)</td>
<td>• 6PE—A technique that provides global IPv6 reachability over IPv4 MPLS. It allows one shared routing table for all other devices. 6PE allows IPv6 domains to communicate with one another over the IPv4 without an explicit tunnel setup, requiring only one IPv4 address per IPv6 domain.</td>
</tr>
<tr>
<td>• IPv6 VPN Provider Edge over MPLS (6VPE)</td>
<td>• 6VPE—A mechanism to use the IPv4 backbone to provide VPN IPv6 services. 6VPE is like a regular IPv4 MPLS-VPN provider edge, with an addition of IPv6 support within VRF. It provides logically separate routing table entries for VPN member devices.</td>
</tr>
</tbody>
</table>

See [Multiprotocol Label Switching](#).

(Network Advantage)
**Programmability**

- Model-Driven Telemetry
- Preboot Execution Environment Client (iPXE)
- YANG Data Models

Programmability features introduced or enhanced in this release:

- ZTP—Now supports HTTP file download along with TFTP file download.
- Model-Driven Telemetry—Provides a mechanism to stream data from a Model-Driven Telemetry-capable device, to a destination. The data to be streamed is driven through subscription. The feature is enabled automatically, when NETCONF-YANG is started on a device.
- iPXE—An open Preboot eXecution Environment (PXE) client that allows a device to boot from a network boot image. iPXE is supported with IPv4 only.
- YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1661.

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.


**Software Maintenance Upgrade (SMU)**

SMU is a package that can be installed on a system, to provide a patch fix or security resolution to a released image.

See System Management -> Software Maintenance Upgrade.

**Stateful Switchover (SSO) Support for IPv6**

SSO is now supported for IPv6 traffic.

With this feature, when an active switch fails, the standby switch starts up in a fully-initialized state and synchronizes with the persistent configuration and the running configuration of the active switch. The new active switch uses existing Layer 2 switching information to continue forwarding traffic.

See High Availability -> Configuring NSF with SSO.

**Virtual Private Network Routing and Forwarding-Aware (VRF-Aware) Generic Routing Encapsulation (GRE)**

Enables you to configure the source and destination of a GRE IP tunnel to belong to any VRF table.

See Routing -> Configuring Generic Routing Encapsulation (GRE) Tunnel IP Source and Destination VRF Membership.
### Important Notes

The following are the unsupported hardware and software features for the Cisco Catalyst 9500 Series Switches. For the list of supported features, go to [http://www.cisco.com/go/cfn](http://www.cisco.com/go/cfn).

- **Unsupported Hardware Features**
  - The rear USB 3.0 Port
  - Breakout cables and breakout LED

- **Unsupported Software Features:**
  - IPsec with FIPS

The following features are supported on the Cisco Catalyst 3850 Series Switches, but not on the Cisco Catalyst 9500 Series Switches:

- 128-bit and 256-bit AES MACsec (IEEE 802.1AE) host link encryption (downlinks) with MACsec Key Agreement (MKA)
- Audio Video Bridging (including IEEE802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav)
- Bluetooth
- Cisco Plug-in for OpenFlow 1.3
- Gateway Load Balancing Protocol (GLBP)
- IPsec VPN
- Multicast—Bidirectional PIM

### New on the Web User Interface

<table>
<thead>
<tr>
<th>Web UI support for DNS Proxy and troubleshooting</th>
<th>Features introduced and updated on the Web UI in this release:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• DNS Proxy Support</td>
</tr>
<tr>
<td></td>
<td>• Troubleshooting- Audit Device Configuration</td>
</tr>
<tr>
<td></td>
<td>• Troubleshooting- Debug Bundle</td>
</tr>
</tbody>
</table>

**Web UI support for DNS Proxy and troubleshooting:**

- DNS Proxy Support
- Troubleshooting- Audit Device Configuration
- Troubleshooting- Debug Bundle

---

### Important Notes

The following are the unsupported hardware and software features for the Cisco Catalyst 9500 Series Switches. For the list of supported features, go to [http://www.cisco.com/go/cfn](http://www.cisco.com/go/cfn).

- **Unsupported Hardware Features**
  - The rear USB 3.0 Port
  - Breakout cables and breakout LED

- **Unsupported Software Features:**
  - IPsec with FIPS

The following features are supported on the Cisco Catalyst 3850 Series Switches, but not on the Cisco Catalyst 9500 Series Switches:

- 128-bit and 256-bit AES MACsec (IEEE 802.1AE) host link encryption (downlinks) with MACsec Key Agreement (MKA)
- Audio Video Bridging (including IEEE802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav)
- Bluetooth
- Cisco Plug-in for OpenFlow 1.3
- Gateway Load Balancing Protocol (GLBP)
- IPsec VPN
- Multicast—Bidirectional PIM
Supported Hardware

Cisco Catalyst 9500 Series Switches—Model Numbers

Table 1 lists the supported hardware models and the default license levels they are delivered with.

The Base PIDs are the model numbers of the switch.

The 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` on such a (bundled PID) switch displays its base PID.

More information about licensing is in section License Levels, page 29

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Default License</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base PIDs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C9500-12Q-E</td>
<td>Network Essentials</td>
<td>12 40-Gigabit Ethernet QSFP ports and two power supply slots</td>
</tr>
<tr>
<td>C9500-12Q-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>C9500-24Q-E</td>
<td>Network Essentials</td>
<td>Cisco Catalyst 9500 Series 24-Port 40 Gigabit Ethernet</td>
</tr>
<tr>
<td>C9500-24Q-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>C9500-40X-E</td>
<td>Network Essentials</td>
<td>40 10-Gigabit Ethernet SFP ports and two power supply slots; support for optional network modules on uplink ports — 8-Port 10 Gigabit Ethernet(SFP) and 2-Port 40 Gigabit Ethernet(QSFP)</td>
</tr>
<tr>
<td>C9500-40X-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>Bundled PIDs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C9500-40X-2Q-E</td>
<td>Network Essentials</td>
<td>40 10-Gigabit Ethernet SFP ports and a 2-Port 40-Gigabit Ethernet (QSFP) network module on uplink ports; and two power supply slots</td>
</tr>
<tr>
<td>C9500-40X-2Q-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>C9500-48X-E</td>
<td>Network Essentials</td>
<td>40 10-Gigabit Ethernet SFP ports and an 8-Port 10-Gigabit Ethernet (SFP) network module on uplink ports; and two power supply slots</td>
</tr>
<tr>
<td>C9500-48X-E</td>
<td>Network Advantage</td>
<td></td>
</tr>
</tbody>
</table>

1. See Table 8 Permitted Combinations, for information about the add-on licenses that you can order

Optics Modules

Catalyst switches support a wide range of optics. Because the list of supported optics is updated on a regular basis, consult the tables at this URL for the latest (SFP) compatibility information:

## Compatibility Matrix

### Table 2  Software Compatibility Matrix

<table>
<thead>
<tr>
<th>Catalyst 9500</th>
<th>Cisco Identity Services Engine</th>
<th>Cisco Access Control Server</th>
<th>Prime Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everest 16.6.7</td>
<td>2.2</td>
<td>5.4</td>
<td>PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Everest 16.6.6</td>
<td>2.2</td>
<td>5.4</td>
<td>PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Everest 16.6.5</td>
<td>2.2</td>
<td>5.4</td>
<td>PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Everest 16.6.4a</td>
<td>2.2</td>
<td>5.4</td>
<td>PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Everest 16.6.4</td>
<td>2.2</td>
<td>5.4</td>
<td>PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Everest 16.6.3</td>
<td>2.2</td>
<td>5.4</td>
<td>PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Everest 16.6.2</td>
<td>2.2</td>
<td>5.4</td>
<td>PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Everest 16.6.1</td>
<td>2.2</td>
<td>5.4</td>
<td>PI 3.1.6 + Device Pack 13 See Prime Infrastructure 3.1 on cisco.com.</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Everest 16.5.1a</td>
<td>2.1 Patch 3</td>
<td>5.4</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Web UI System Requirements

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

Hardware Requirements

<table>
<thead>
<tr>
<th>Processor Speed</th>
<th>DRAM</th>
<th>Number of Colors</th>
<th>Resolution</th>
<th>Font Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>233 MHz minimum¹</td>
<td>512 MB²</td>
<td>256</td>
<td>1024 x 768</td>
<td>Small</td>
</tr>
</tbody>
</table>

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

Software Requirements

- Operating Systems
  - Windows 10 or later
  - Mac OS X 10.11 or later

- Browsers
  - Google Chrome—Version 38 and later (On Windows and Mac)
  - Microsoft Internet Explorer—Version 11 or later (On Windows 7 and Windows XP), and Microsoft Edge (On Windows 10)
  - Mozilla Firefox—Version 33 and later (On Windows and Mac)
  - Safari—Version 7 and later (On Mac)

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.
Upgrading the Switch Software

**Note**
You cannot use the Web UI to install, upgrade, or downgrade switch software

This section covers the following:
- Automatic Boot Loader Upgrade
- Upgrading in Install Mode
- Downgrading in Install Mode

**Note**
From Cisco IOS XE Everest 16.6.2 onwards, we support new `install` commands. These `install` commands are supported along with the previously supported `request platform software` commands. Both set of commands are supported at present.

---

### Table 4 Software Images

<table>
<thead>
<tr>
<th>Release</th>
<th>Image</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.7</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.07.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.07.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.6</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.06.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.06.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.5</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.05.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.05.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.4a</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.04a.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.04a.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.4</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.04.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.04.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.3</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.03.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.03.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.2</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.02.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.02.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.01.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.01.SPA.bin</td>
</tr>
</tbody>
</table>
Upgrading the Switch Software

Table 5  request platform software Commands to Upgrade or Downgrade Switch Software

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clean</td>
<td>Cleans unnecessary package files from media.</td>
</tr>
<tr>
<td>copy</td>
<td>Copies package to media.</td>
</tr>
<tr>
<td>describe</td>
<td>Describes package contents.</td>
</tr>
<tr>
<td>expand</td>
<td>Expands all-in-one package to media.</td>
</tr>
<tr>
<td>install</td>
<td>Installs package.</td>
</tr>
<tr>
<td>uninstall</td>
<td>Uninstalls package.</td>
</tr>
<tr>
<td>verify</td>
<td>Verifies ISSU software package compatibility.</td>
</tr>
</tbody>
</table>

Table 6  install Commands to Upgrade or Downgrade Switch Software

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# install add file filename [activate commit]—Use this command to install and activate the specified file, and to commit changes to be persistent across reloads.</td>
<td></td>
</tr>
<tr>
<td>Switch# install ?—You can also use the install command to separately install, activate, commit, abort, or remove the installation file.</td>
<td></td>
</tr>
<tr>
<td>add file tftp: filename</td>
<td>Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.</td>
</tr>
<tr>
<td>activate</td>
<td>Activates the file, and reloads the device. The auto-abort-timer keyword automatically rolls back the image activation.</td>
</tr>
<tr>
<td>commit</td>
<td>Makes changes persistent over reloads.</td>
</tr>
<tr>
<td>rollback to committed</td>
<td>Rolls back the update to the last committed version.</td>
</tr>
<tr>
<td>abort</td>
<td>Aborts the file activation, and rolls back to the version that was running before the current installation procedure started.</td>
</tr>
<tr>
<td>remove</td>
<td>Deletes all unused and inactive software installation files.</td>
</tr>
</tbody>
</table>

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 IOS XE 16.x.x releases, if there is a new boot loader 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.
Upgrading in Install Mode

Follow these instructions to upgrade from one release to another, in install mode.

In Cisco IOS XE Everest 16.6.2, a new set of **install** commands have been introduced for the install and upgrade of images in install mode. You can either use the **install** commands or the **request platform software** commands for install, upgrade, and downgrade of software images. For more information, see the Software Install chapter of the *System Management Configuration Guide*.

**Note**

The **install** commands are available only from Cisco IOS XE Everest 16.6.2.

The sample output in this section covers upgrade from Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Everest 16.6.1 and from Cisco IOS XE Everest 16.6.1 to Cisco IOS XE Everest 16.6.2 in Install Mode. This section provides examples of both **request platform software** and **install** commands.
Clean Up

Step 1
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. The following sample output displays the cleaning up of Cisco IOS XE Everest 16.5.1a files.

```
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.
  packages.conf
      File is in use, will not delete.
  done.

The following files will be deleted:
[1]:
  /flash/cat9k-cc_srdriver.2017-07-26_17.04.SPA.pkg
  /flash/cat9k-espbase.2017-07-26_17.04.SPA.pkg
  /flash/cat9k-guestshell.2017-07-26_17.04.SPA.pkg
  /flash/cat9k-rpbase.2017-07-26_17.04.SPA.pkg
  /flash/cat9k-rpboot.2017-07-26_17.04.SPA.pkg
  /flash/cat9k-sipbase.2017-07-26_17.04.SPA.pkg
  /flash/cat9k-sipspa.2017-07-26_17.04.SPA.pkg
  /flash/cat9k-srdriver.2017-07-26_17.04.SPA.pkg
  /flash/cat9k-webui.2017-07-26_17.04.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.2017-07-26_17.04.SPA.pkg ... done.
  Deleting file flash:cat9k-espbase.2017-07-26_17.04.SPA.pkg ... done.
  Deleting file flash:cat9k-guestshell.2017-07-26_17.04.SPA.pkg ... done.
  Deleting file flash:cat9k-rpbase.2017-07-26_17.04.SPA.pkg ... done.
```

Summary Steps—Clean Up > Copy New Image to Flash > Set Boot Variable> Set Boot Variable > Reload
Deleting file flash:cat9k-rpboot.2017-07-26_17.04.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.2017-07-26_17.04.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.2017-07-26_17.04.SPA.pkg ... done.
Deleting file flash:cat9k-webui.2017-07-26_17.04.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#

You can also use the `install remove inactive` command to clean up old installation files in case of insufficient space. The following sample output displays the cleaning up of Cisco IOS XE Everest 16.6.1 files:

Switch# install remove inactive

install_remove: START Mon Oct 30 19:51:48 UTC 2017
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.16.06.01.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-srdriver.16.06.01.SPA.pkg
flash:/cat9k-sipspa.16.06.01.SPA.pkg
flash:/cat9k-webui.16.06.01.SPA.pkg
flash:/cat9k-wlc.16.06.01.SPA.pkg
flash:/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:/cat9k-cc_srdriver.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-srdriver.16.06.01.SPA.pkg ... done.
Deleting file flash:/cat9k-sipspa.16.06.01.SPA.pkg ... done.
Deleting file flash:/cat9k-webui.16.06.01.SPA.pkg ... done.
Deleting file flash:/cat9k-wlc.16.06.01.SPA.pkg ... done.
Deleting file flash:/packages.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
[1] Post_Remove_Cleanup on switch 1
[1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Mon Oct 30 19:52:25 UTC 2017
Switch#
Upgrading the Switch Software

Copy New Image to Flash

Step 2  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 - 601216545 bytes]
601216545 bytes copied in 50.649 secs (11870255 bytes/sec)

Step 3  Use the dir flash command to confirm that the image has been successfully copied to flash.

Switch# dir flash:*.bin
Directory of flash:/*.bin
Directory of flash:/
434184 -rw- 601216545 Jul 26 2017 10:18:11 -07:00 cat9k_iosxe.16.06.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)

Set Boot Variable

Step 4  Use the boot system flash:packages.conf command to set the boot variable.

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

Use the write memory command to save boot settings.

Switch# write memory

Use this command to verify BOOT variable = flash:packages.conf

Switch# show boot system

Software Install Image to Flash

Use the request platform software package install switch all file flash: command to install the target image to flash. You can point to the source image on your TFTP server or in flash if you have it copied to flash.

Note  On a device where the Cisco StackWise Virtual feature is configured, we recommend copying the image to a TFTP server or the flash drive of the active switch. If you point to an image on the flash or USB drive of the standby (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For example, if the image is on the flash drive of standby switch 2(flash-2):

Switch# request platform software package install switch all file flash-2:cat9k_iosxe.16.06.01.SPA.bin
<output truncated>
Expanding image file: flash-2: cat9k_iosxe.16.06.01.SPA.bin
[3]: Copying flash-2: cat9k_iosxe.16.06.01.SPA.bin from switch 2 to switch 1
<output truncated>
The following example displays the installation of Cisco IOS XE Everest 16.6.1 software image:

Switch# request platform software package install switch all file flash:cat9k_iosxe.16.06.01.SPA.bin

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

Expanding image file: flash:cat9k_iosxe.16.06.01.SPA.bin
[1]: 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]: 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.16.06.01a.SPA.pkg
Added cat9k-espbase.16.06.01a.SPA.pkg
Added cat9k-guestshell.16.06.01a.SPA.pkg
Added cat9k-rpbase.16.06.01a.SPA.pkg
Added cat9k-rpboot.16.06.01a.SPA.pkg
Added cat9k-sipbase.16.06.01a.SPA.pkg
Added cat9k-sipspa.16.06.01a.SPA.pkg
Added cat9k-srdriver.16.06.01a.SPA.pkg
Added cat9k-webui.16.06.01a.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[1]: Performing 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 will not be removed from flash.

You can also use the install add file activate commit command to install the target image to flash. This example displays the upgrade to Cisco IOS XE Everest 16.6.2.

Switch# install add file flash:cat9k_iosxe.16.06.02.SPA.bin activate commit

install_add_activate_commit: START Mon Oct 30 19:54:51 UTC 2017

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

install_engine.sh: %INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.06.02.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.16.06.02.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:/flash/cat9k-wlc.16.06.02.SPA.pkg
flash:/flash/cat9k-webui.16.06.02.SPA.pkg
flash:/flash/cat9k-srdriver.16.06.02.SPA.pkg
flash:/flash/cat9k-sipspa.16.06.02.SPA.pkg
flash:/flash/cat9k-sipbase.16.06.02.SPA.pkg
flash:/flash/cat9k-rpboot.16.06.02.SPA.pkg
flash:/flash/cat9k-rpbase.16.06.02.SPA.pkg
flash:/flash/cat9k-guestshell.16.06.02.SPA.pkg
flash:/flash/cat9k-espbase.16.06.02.SPA.pkg
flash:/flash/cat9k-cc_srdriver.16.06.02.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

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  Mon Oct 30 19:57:48 UTC 2017
Switch#

Note: The system reloads automatically after executing the install add file activate commit command. There is no need to manually reload the system.
Step 5  After the software has been successfully installed, verify that the flash partition has nine new .pkg files and three .conf files. See sample output below. The following is sample output from the `dir flash:` command in Cisco IOS XE Everest 16.6.1:

```
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 09:53:02 -07:00 cat9k-rpbase.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
516099 -rw- 5297096 Oct 30 2017 10:57:44 -07:00 cat9k-cc_srdriver.16.06.01.SPA.pkg
516100 -rw- 80946116 Oct 30 2017 10:57:46 -07:00 cat9k-espbase.16.06.01.SPA.pkg
516101 -rw- 1536964 Oct 30 2017 10:57:47 -07:00 cat9k-guestshell.16.06.01.SPA.pkg
516102 -rw- 376865728 Oct 30 2017 10:57:57 -07:00 cat9k-rpbase.16.06.01.SPA.pkg
516107 -rw- 27669444 Oct 30 2017 10:57:58 -07:00 cat9k-sipbase.16.06.01.SPA.pkg
516104 -rw- 55440320 Oct 30 2017 10:58:00 -07:00 cat9k-sipspa.16.06.01.SPA.pkg
516103 -rw- 29545049 Oct 30 2017 10:58:08 -07:00 cat9k-rpboot.16.06.01.SPA.pkg
516105 -rw- 11813828 Oct 30 2017 10:58:00 -07:00 cat9k-srdriver.16.06.01.SPA.pkg
516106 -rw- 12248000 Oct 30 2017 10:58:00 -07:00 cat9k-webui.16.06.01.SPA.pkg

11353194496 bytes total (8963174400 bytes free)
```

The following is sample output from the `dir flash:` command in Cisco IOS XE Everest 16.6.2:

```
Switch# dir flash:
Directory of flash:/
253956  -rw-   2097152 Nov 3  2017 21:37:04  -07:00 nvram_config
253955  -rw-   2097152 Nov 3  2017 21:37:04  -07:00 nvram_config_bkup
253954  -rw-       239 Nov 3  2017 21:28:47  -07:00 boothelper.log
253957  -rw-        78 Oct 27 2017 14:28:43  -07:00 tam_client_app.log
303111  -rw-  5297096 Nov 1  2017 23:27:26 -07:00 cat9k-cc_sddriver.16.06.01.SPA.pkg
253961  -rw-      7523 Nov 1  2017 23:56:25 -07:00 packages.conf
344067  -rw-   5186504 Nov 1  2017 23:54:10 -07:00 cat9k-cc_sddriver.16.06.02.SPA.pkg
303112  -rw-  80946116 Nov 1  2017 23:27:29 -07:00 cat9k-espbase.16.06.01.SPA.pkg
303113  -rw-  1536964 Nov 1  2017 23:27:29 -07:00 cat9k-guestshell.16.06.02.SPA.pkg
303118  -rw-  29545049 Nov 1  2017 23:27:53 -07:00 cat9k-rpboot.16.06.01.SPA.pkg
303114  -rw-  27669444 Nov 1  2017 23:27:41 -07:00 cat9k-sipbase.16.06.01.SPA.pkg
294913 drwx  4096 Nov 3  2017 21:28:25 -07:00 .installer
253966  -rw-  16280 Nov 3  2017 21:28:42 -07:00 bootloader_evt_handle.log
303105 drwx  4096 Oct 26 2017 20:57:12 -07:00 core
311297 drwx  4096 Oct 26 2017 20:57:12 -07:00 .prst_sync
327681 drwx  4096 Nov 1  2017 23:56:42 -07:00 rollback_timer
335873 drwx  4096 Nov 1  2017 23:56:46 -07:00 dc_profile_dir
335875 drwx  4096 Oct 26 2017 20:48:50 -07:00 gs_script
253959  -rw-  556 Nov 1  2017 23:42:12 -07:00 vlan.dat
253968  -rw-  98869 Nov 3  2017 21:28:59 -07:00 memleak.tcl
294914 drwx  4096 Oct 26 2017 21:19:34 -07:00 tech_support
303107 drwx  4096 Oct 26 2017 21:27:19 -07:00 onep
319490 drwx  4096 Oct 26 2017 21:27:19 -07:00 CRDU
303115  -rw-  55440320 Nov 1  2017 23:27:43 -07:00 cat9k-sipspa.16.06.01.SPA.pkg
303116  -rw-  11813828 Nov 1  2017 23:27:43 -07:00 cat9k-srdriver.16.06.01.SPA.pkg
303117  -rw-  12248000 Nov 1  2017 23:27:43 -07:00 cat9k-webui.16.06.01.SPA.pkg
```
In the following sample output that 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.
- packages.conf.00 — backup file of the previously installed image.
- cat9k_iosxe.16.06.01.SPA.conf — a copy of packages.conf and not used by the system.

Switch# dir flash:*.conf

Directory of flash:/.*.conf

Directory of flash: /

434197 -rw- 7406 Jul 26 2017 10:59:16 -07:00 packages.conf
434196 -rw- 7504 Jul 26 2017 10:59:16 -07:00 packages.conf.00
516098 -rw- 7406 Jul 26 2017 10:58:08 -07:00 cat9k_iosxe.16.06.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)

Reload

Step 6  Reload the switch

Switch# reload

Step 7  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

When the new image boots up, verify the version of the new image, using the show version command:

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

The following 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, RELEASESOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Sat 22-Jul-17 05:51 by mcpp
The following `show version` command displays the Cisco IOS XE Everest 16.6.2 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.06.02
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.6.2, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Sat 28-Oct-17 06:38 by mcpree
```

## Downgrading in Install Mode

**Note**

New switch models that are introduced in a release cannot be downgraded, so if you add a new switch to an existing stack, we recommend upgrading all existing switches. For the list of models introduced in a release, see the list of hardware features in that release.

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

The sample output in this section covers downgrade from Cisco IOS XE Everest 16.6.1 to Cisco IOS XE Everest 16.5.1a and from Cisco IOS XE Everest 16.6.2 to Cisco IOS XE Everest 16.6.1 in Install Mode.

This section provides examples of both `request platform software` and `install` commands.

**Summary Steps—Clean Up > Copy New Image to Flash > Downgrade Software Image > Reload**

### Clean Up

**Step 1**

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. The following sample output displays the cleaning up of Cisco IOS XE Everest 16.6.1 files:

```
Switch# request platform software package clean
This operation may take several minutes...
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.16.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-espbase.16.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-guestshell.16.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpbase.16.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpboot.16.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipbase.16.06.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipspa.16.06.01.SPA.pkg
      File is in use, will not delete.
```
Upgrading the Switch Software

Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Everest 16.6.x

You can also use the `install remove inactive` command to clean up old installation files in case of insufficient space. The following sample output displays the cleaning up of Cisco IOS XE Everest 16.6.2 files:

```
  Switch# install remove inactive

  install_remove: START Mon Oct 30 19:51:48 UTC 2017
  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.16.06.02.SPA.pkg
  /flash/cat9k-espbase.16.06.02.SPA.pkg
  /flash/cat9k-guestshell.16.06.02.SPA.pkg
  /flash/cat9k-rpbase.16.06.02.SPA.pkg
  /flash/cat9k-rpboot.16.06.02.SPA.pkg
  /flash/cat9k-sipbase.16.06.02.SPA.pkg
  /flash/cat9k-sipspa.16.06.02.SPA.pkg
  /flash/cat9k-srdriver.16.06.02.SPA.pkg
  /flash/cat9k-webui.16.06.02.SPA.pkg
  /flash/cat9k-wlc.16.06.02.SPA.pkg
  /flash/cat9k_iosxe.16.06.01.SPA.conf
  /flash/packages.conf
```

The following files will be deleted:

- `cat9k-srdriver.16.06.01.SPA.pkg`
  File is in use, will not delete.
- `cat9k-webui.16.06.01.SPA.pkg`
  File is in use, will not delete.
- `packages.conf`
  File is in use, will not delete.

 done.

Do you want to proceed? [y/n] y

[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-iosxe.16.06.01.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
Do you want to remove the above files? [y/n] y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-siplspa.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.02.SPA.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
   [1] Post_Remove_Cleanup package(s) on switch 1
   [1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup
SUCCESS: install_remove  Mon Oct 30 19:52:25 UTC 2017
Switch#

Copy New Image to Flash

Step 2  Copy the target Cisco IOS XE Everest 16.5.1a image to flash: (you can skip this step if you want to use the image from your TFTP server).
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.05.01a.SPA.bin flash:
Destination filename [cat9k_iosxe.16.05.01a.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.05.01a.SPA.bin...
Loading /cat9k_iosxe.16.05.01a.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 508584771 bytes]
508584771 bytes copied in 101.005 secs (5035244 bytes/sec)

Step 3  Use the dir flash command to confirm that the image has been successfully copied to flash.
Switch# dir flash:*.bin
Directory of flash:/*.bin

Directory of flash:/

434184  -rw- 508584771 Jul 26 2017 13:35:16 -07:00 cat9k_iosxe.16.05.01a.SPA.bin
11353194496 bytes total (9055866880 bytes free)
Downgrade Software Image

Step 4  Use the `request platform software package install` command, to downgrade your stack. You can point to the source image on your tftp server or in flash if you have it copied to flash. The following example displays the installation of Cisco IOS XE Everest 16.5.1a software image:

```
Switch# request platform software package install switch all file flash:cat9k_iosxe.16.05.01a.SPA.bin

--- Starting install local lock acquisition on switch 1 ---
Finished install local lock acquisition on switch 1
Expanding image file: flash:cat9k_iosxe.16.05.01a.SPA.bin
[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.16.06.01.SPA.pkg
  Removed cat9k-espbase.16.06.01.SPA.pkg
  Removed cat9k-guestshell.16.06.01.SPA.pkg
  Removed cat9k-rpbase.16.06.01.SPA.pkg
  Removed cat9k-rpboot.16.06.01.SPA.pkg
  Removed cat9k-sipbase.16.06.01.SPA.pkg
  Removed cat9k-sipspa.16.06.01.SPA.pkg
  Removed cat9k-webui.16.06.01.SPA.pkg
New files list:
  Added cat9k-cc_srdriver.16.05.01a.SPA.pkg
  Added cat9k-espbase.16.05.01a.SPA.pkg
  Added cat9k-guestshell.16.05.01a.SPA.pkg
  Added cat9k-rpbase.16.05.01a.SPA.pkg
  Added cat9k-rpboot.16.05.01a.SPA.pkg
  Added cat9k-sipbase.16.05.01a.SPA.pkg
  Added cat9k-sipspa.16.05.01a.SPA.pkg
  Added cat9k-webui.16.05.01a.SPA.pkg
  Added cat9k-wlc.16.05.01a.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]
```

You can also use the `install add file activate commit` command to install the target image to flash. This example displays the installation of Cisco IOS XE Everest 16.6.1:

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

install_add_activate_commit: START Mon Oct 30 19:54:51 UTC 2017

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

[OK]Modified configuration has been saved
```
Upgrading the Switch Software

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

rollback_timer.sh: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGESS: 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 Mon Oct 30 19:57:48 UTC 2017

Switch#

Note
The system reloads automatically after executing the **install add file activate commit** command. There is no need to manually reload the system.
Reload

Step 5  Reload the switch

Switch# reload

Step 6  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

Step 7  When the new image boots up, you can verify the version of the new image, by checking show version

**Note**  In the output, note that the boot loader is not automatically downgraded.

The following `show version` command displays the Cisco IOS XE Everest 16.5.1a image on the device:

Switch# show version

Cisco IOS XE Software, Version 16.05.01a
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.5.1a, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Tue 30-May-17 00:36 by mcpre

The following `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 Sat 28-Oct-17 06:38 by mcpre
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 fall under the base or add-on license levels.

Base Licenses

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

Add-On Licenses—Require a Network Essentials or Advantage as a prerequisite. 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—including 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 http://www.cisco.com/go/cfn. 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—for a license level, preinstalled on the device, and for a 90-day trial period only.

Ordering with Smart Accounts

We recommend that you use Smart Accounts to order devices as well as licenses. Smart Accounts enable you to manage all of your software licenses for switches, routers, firewalls, access-points or tools from one centralized website. To create Smart Accounts, use the Cisco Smart Software Manager (Cisco SSM).

Note

This is especially relevant to the term licenses that you order, because information about the expiry of term licenses is available only through the Cisco SSM website.

For information more information about Cisco SSM, see:

The possible deployment modes are:

- Right-to-use (RTU) licensing mode—Supported on Cisco Catalyst 9000 Series Switches, in Cisco IOS XE Everest 16.5.1a. See The RTU Licensing Mode, page 30.
- Smart Licensing mode—Currently not supported on Cisco Catalyst 9000 Series Switches. It is on the roadmap for future releases.

## The RTU Licensing Mode

This is the currently supported licensing mode for Cisco Catalyst 9000 Series Switches.

Right-to-use (RTU) licensing allows you to order and activate a specific license type for a given license level, and then to manage license usage on your switch.

**Note**  The RTU licensing structure has been modified to match the packaging model that will be used with Smart Licensing mode in the future. Unified licensing structures across the RTU and Smart Licensing modes, along with usage reports, will simplify migration and reduce the implementation time required for Smart Licensing.

The *license right-to-use* command (privilege EXEC mode) provides options to activate or deactivate any license supported on the platform.

### Options for Base Licenses

```
license right-to-use [activate | deactivate] [network-essentials | network-advantage] [all | evaluation | subscription {all | slot <1-8>} ] [acceptEULA]
```

### Options for Add-On Licenses

```
license right-to-use [activate | deactivate] addon [dna-essentials | dna-advantage] [all | evaluation | subscription {all | slot <1-8>} ] [acceptEULA]
```

## Usage Guidelines for the RTU Licensing Mode

- Licenses may be activated on a standalone device.
- Base licenses (Network Essentials and Network-Advantage) may be ordered only with a permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) may be ordered only with a term license type.

You can set up Cisco SSM to receive daily e-mail alerts, to be notified of expiring add-on licenses that you want to renew.

You must order an add-on license in order to purchase a switch. On term expiry, you can either renew the add-on license 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 8  Permitted Combinations

<table>
<thead>
<tr>
<th></th>
<th>DNA Essentials</th>
<th>DNA Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Essentials</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Network Advantage</td>
<td>Yes&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<sup>1</sup> For this combination, the DNA-Essentials license must be ordered separately using Cisco SSM.
• The following features are currently available only at the Network Advantage license level. However, the correct minimum license level for these features is Network Essentials and the CFN reflects this correct license level.
  
  You will be able to configure the feature with a Network Essentials license level after the correction is made in an upcoming release.
  
  – IPv6 Multicast
  
  – IPv6 ACL Support for HTTP Servers

• Evaluation licenses cannot be ordered. They can be activated temporarily, without purchase. Warning system messages about the evaluation license expiry are generated 10 and 5 days before the 90-day window. Warning system messages are generated every day after the 90-day period. An expired evaluation license cannot be reactivated after reload.

For more information about using the RTU Licensing Mode, see the System Management > Configuring Right-To-Use Licenses chapter in the software configuration guide.

Scaling Guidelines

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


Limitations and Restrictions

• Hardware
  
  – Use the MODE button to switch-off the beacon LED.
  
  – All port LED behavior is undefined until interfaces are fully initialized.

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

• Control Plane Policing (CoPP)—Starting with Cisco IOS XE Everest 16.6.4, 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 (FNF) 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, and tunnels.

• You can not configure multiple flow monitors of the same type (ipv4, ipv6 or datalink) on the same interface, and in the same direction.

• Hardware limitations:
Limitations and Restrictions

- For all the devices running Cisco IOS XE Everest 16.6.1 or Cisco IOS XE Everest 16.6.2 or Cisco IOS XE Everest 16.6.3, autonegotiation is disabled by default when you use Cisco 40GBASE-CR4 QSFP Direct-Attach Copper Cables. If the other end of the link has autonegotiation enabled, the link does not come up.

  **Note** There is no option to turn on autonegotiation on the ports which connect to Cisco 40GBASE-CR4 QSFP cable.

- For all the Catalyst 9500 Series Switches running Cisco IOS XE Everest 16.6.4 and later, autonegotiation is enabled by default when you use Cisco 40GBASE-CR4 QSFP Direct-Attach Copper Cables. If the other end of the link does not support autonegotiation, the link does not come up. You can turn autonegotiation off on the ports which connect to Cisco 40GBASE-CR4 QSFP cable. Use the `speed nonegotiate` command at the interface. This command disables autonegotiation and brings the link up. To restore autonegotiation, use the `no speed nonegotiate` command.

- Interoperability limitations:
  - If one end of the link has a device running Cisco IOS XE Everest 16.6.1 or Cisco IOS XE Everest 16.6.2 or Cisco IOS XE Everest 16.6.3 and the other end is running Cisco IOS XE Fuji 16.8.1, the link does not come up. To avoid this interoperability issue between releases, it is recommended to use the same image across all the Catalyst 9300 Series Switches and Catalyst 9500 Series Switches in the network.

- Memory leak—When a logging discriminator is configured and applied to a device, memory leak is seen under heavy syslog or debug output. The rate of the leak is dependent on the quantity of logs produced. In extreme cases, the device may fail. As a workaround, disable the logging discriminator on the device.

- QoS restrictions:
  - When configuring a QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - For QoS policies, only SVIs 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 (Secure Copy Protocol) and SSH cryptographic operations, expect high CPU until the SCP read process is completed. SCP supports file transfers between hosts on a network and uses SSH for the transfer.

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

- Smart Install—The feature is deprecated starting with Cisco IOS XE Everest 16.5.1a. The commands are visible on the CLI until Cisco IOS XE Everest 16.6.1, but the feature is not supported. Enter the `no vstack` command in global configuration mode and disable the feature. Starting from Cisco IOS XE Everest 16.6.2, the `vstack` command is not available on the CLI.

- Wired AVC 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 attributes based QoS is not supported (‘match protocol attribute’).
- 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
- **VLAN Restriction:** It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.
- **YANG data modeling limitations**—A maximum of 20 simultaneous NETCONF sessions are supported.
Caveats

Caveats describe unexpected behavior in Cisco IOS 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, page 34
- Open Caveats in Cisco IOS XE Everest 16.6.x, page 34
- Resolved Caveats in Cisco IOS XE Everest 16.6.5, page 36
- Resolved Caveats in Cisco IOS XE Everest 16.6.4a, page 38
- Resolved Caveats in Cisco IOS XE Everest 16.6.4, page 38
- Resolved Caveats in Cisco IOS XE Everest 16.6.3, page 40
- Resolved Caveats in Cisco IOS XE Everest 16.6.2, page 40
- Resolved Caveats in Cisco IOS XE Everest 16.6.1, page 40

Cisco Bug Search Tool

The 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 Everest 16.6.x

The following are the open caveats in this release:

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvk60809</td>
<td>Wrong Time-Stamp is saved in pcap.</td>
</tr>
<tr>
<td>CSCvq13055</td>
<td>NAT translation entry not cleared after fin-rst time-out</td>
</tr>
<tr>
<td>CSCvq72713</td>
<td>Cat3k/Cat9k can't forwarding traffic follow the rule of EIGRP unequal cost load-balancing</td>
</tr>
<tr>
<td>CSCvr21001</td>
<td>QoS with policing traffic that do not match the ACL on the class-map</td>
</tr>
<tr>
<td>CSCvr21641</td>
<td>Default command doesn't work for not connect port.</td>
</tr>
<tr>
<td>CSCvh72186</td>
<td>ROMMON: HTTP booting does not allow specified port number</td>
</tr>
</tbody>
</table>
# Resolved Caveats in Cisco IOS XE Everest 16.6.7

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvq72181</td>
<td>Seeing 100% CPU with FED on SVL setup</td>
</tr>
<tr>
<td>CSCvf42299</td>
<td>User defined System MTU is not taking effect on PO and SVI</td>
</tr>
<tr>
<td>CSCvj16691</td>
<td>Port LED may turn to amber</td>
</tr>
<tr>
<td>CSCvm89543</td>
<td>StackWise-Virtual Ping fails momentarily due to GLC-T optics Link goes up during reboots</td>
</tr>
<tr>
<td>CSCvn30230</td>
<td>Slow memory leak in linux_iosd_imag</td>
</tr>
<tr>
<td>CSCvn81334</td>
<td>Default ACL being enforced even when dACL is applied after Reload</td>
</tr>
<tr>
<td>CSCvo65974</td>
<td>QinQ tunnels causing L2 loop in specific topology.</td>
</tr>
<tr>
<td>CSCvo71264</td>
<td>Gateway routes DHCP offer incorrectly after DHCP snooping</td>
</tr>
<tr>
<td>CSCvo83305</td>
<td>MAC Access List Blocks Unintended Traffic</td>
</tr>
<tr>
<td>CSCvo85183</td>
<td>Uplinkfast take time when recovery from link failure</td>
</tr>
<tr>
<td>CSCvo85422</td>
<td>Directly connected IPv4/IPv6 hosts not programmed in HW - %FMFP-3-OBJ_DWNLD_TO_DP FAILED</td>
</tr>
<tr>
<td>CSCvo94058</td>
<td>URPF packet drop despite &quot;rx allow-default&quot; option</td>
</tr>
<tr>
<td>CSCvp00026</td>
<td>No audio during first few seconds of voice call between 2 Fabric Edge</td>
</tr>
<tr>
<td>CSCvp15389</td>
<td>Port security configuration on interface causing connectivity issue</td>
</tr>
<tr>
<td>CSCvp26792</td>
<td>Control plane impacted when &gt; 1Gbps multicast passes through and no entry in IGMP snooping</td>
</tr>
<tr>
<td>CSCvp30239</td>
<td>Memory leak when there are constant changes in REP ring</td>
</tr>
<tr>
<td>CSCvp33294</td>
<td>Asic 0 Core 0 buffer stuck, rwePbcStall seen</td>
</tr>
<tr>
<td>CSCvp43131</td>
<td>Mgmt port &quot;speed 1000&quot; and &quot;negotiation auto&quot; in show run</td>
</tr>
<tr>
<td>CSCvp54779</td>
<td>[SDA] 1st ARP Reply is dropped at remote Fabric Edge</td>
</tr>
<tr>
<td>CSCvp69629</td>
<td>Authentication sessions does not come up on configuring dot1x when there is active client traffic.</td>
</tr>
<tr>
<td>CSCvp75221</td>
<td>Modules shows faulty status when specific MAC ACL is applied on interfaces</td>
</tr>
<tr>
<td>CSCvp89755</td>
<td>VPN label is wrongly derived as explicit-null in Cat9k for L3 VPN traffic</td>
</tr>
<tr>
<td>CSCvp90279</td>
<td>ADV and REP DHCPv6 packets are sent to SISF when source udp port is not 547</td>
</tr>
<tr>
<td>CSCvq01185</td>
<td>SNMP-3-RESPONSE_DELAYED: and timeout when polling ent Sensor Value Entry</td>
</tr>
<tr>
<td>CSCvq22011</td>
<td>ARP replies are dropped when IPDT gleans from ARP</td>
</tr>
<tr>
<td>CSCvq30316</td>
<td>[SDA] 1st ARP fix for CSCvp00026 is eventually failing after longevity</td>
</tr>
<tr>
<td>CSCvq30460</td>
<td>SYS-2-BADSHARE: Bad refcount in datagram_done - messages seen during system churn</td>
</tr>
<tr>
<td>CSCvq40137</td>
<td>Mac address not being learnt when &quot;auth port-control auto&quot; command is present</td>
</tr>
<tr>
<td>CSCvq44397</td>
<td>ospf down upon switchover with aggressive timers &quot;hello-interval 1&quot; and &quot;dead-interval 4&quot;</td>
</tr>
</tbody>
</table>
## Resolved Caveats in Cisco IOS XE Everest 16.6.6

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvn08296</td>
<td>DNA Center 1.2.5 - SDA Border as RP incorrectly resolving RPF next-hop as LISP interface</td>
</tr>
<tr>
<td>CSCvo32446</td>
<td>High CPU Due To Looped Packet and/or Unicast DHCP ACK Dropped</td>
</tr>
<tr>
<td>CSCuw36080</td>
<td>SNMP with Extended ACL</td>
</tr>
<tr>
<td>CSCvg73991</td>
<td>PBR adjacency not getting updated correctly after shut/no shut on interface</td>
</tr>
<tr>
<td>CSCvm07353</td>
<td>Router may crash when a SSH session is closed after configure TACACS</td>
</tr>
<tr>
<td>CSCvm48084</td>
<td>Remark in DACL causes Authorization failure</td>
</tr>
<tr>
<td>CSCvm77197</td>
<td>C9300/9500:%IOSXE-2-PLATFORM: Switch 1 R0/0: kernel: EXT2-fs (sda1): error:</td>
</tr>
<tr>
<td>CSCvm89086</td>
<td>SPAN destination interface not dropping ingress traffic</td>
</tr>
<tr>
<td>CSCvn01822</td>
<td>cmnMacMoveNotification is generated when a MAC address is moved between same Port-channel interface</td>
</tr>
<tr>
<td>CSCvn23706</td>
<td>no mac address-table notification mac-move can't be saved after reload device</td>
</tr>
<tr>
<td>CSCvn31477</td>
<td>Layer 2 SSM Multicast traffic hitting the CPU when SVI is configured with PIM Spare Mode</td>
</tr>
<tr>
<td>CSCvn46517</td>
<td>some sgacl were not installed after update a Cell in ISE</td>
</tr>
<tr>
<td>CSCvn56579</td>
<td>MQIPC memory corruption resulting dot1x/MAB not working for wired clients</td>
</tr>
<tr>
<td>CSCvn72973</td>
<td>Device is getting crashed on the &quot;cts role-based enforcement&quot;</td>
</tr>
<tr>
<td>CSCvn74807</td>
<td>Cisco TrustSec crash while processing CoA update</td>
</tr>
<tr>
<td>CSCvn79221</td>
<td>MAC ADDRESS LEARNING FAILURE ON PORT CONFIGURED WITH PORT-SECURITY</td>
</tr>
<tr>
<td>CSCvo15594</td>
<td>MATM programming issue for remote client</td>
</tr>
<tr>
<td>CSCvo42353</td>
<td>SDA; Cat3K,Cat9K;-External border creating incorrect CEF/map-cache entry due to multicast</td>
</tr>
</tbody>
</table>

## Resolved Caveats in Cisco IOS XE Everest 16.6.5

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvh85885</td>
<td>IPv6 stale entries not expiring</td>
</tr>
<tr>
<td>CSCvi48988</td>
<td>SNMP timeout when querying entSensorValueEntry</td>
</tr>
<tr>
<td>CSCvi96965</td>
<td>Radius Automate Tester probe on feature is not working as expected.</td>
</tr>
<tr>
<td>CSCvj79694</td>
<td>sgt-map gets cleared for some of the end points for unknown reason</td>
</tr>
<tr>
<td>CSCvj92201</td>
<td>16.6.4:Device-tracking does not consistenly show DH4 for DHCP clients</td>
</tr>
<tr>
<td>CSCvk20003</td>
<td>Polaris: Host limit of 32 for session monitoring sessions</td>
</tr>
<tr>
<td>CSCvk30813</td>
<td>MAB fails to start negotiation after device moves to another layer 2 adjacent switch</td>
</tr>
</tbody>
</table>

Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Everest 16.6.x
<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvk32866</td>
<td>SISF probing behavior should be changed from broadcast to unicast</td>
</tr>
<tr>
<td>CSCvk33369</td>
<td>Stack-merge on Stby and CONN_ERR_CONN_TIMEOUT_ERR on Active with multiple SWO</td>
</tr>
<tr>
<td>CSCvk33624</td>
<td>SFF8472-3-READ_ERROR message seen for SVL ports</td>
</tr>
<tr>
<td>CSCvk34927</td>
<td>DHCP snooping table not updated from DHCP snooping DB file upon reload.</td>
</tr>
<tr>
<td>CSCvk39041</td>
<td>SDA: IP phone latency in fabric is close to 4 sec's</td>
</tr>
<tr>
<td>CSCvk60752</td>
<td>DHCP offer with Option 82 but no Remote ID suboption dropped by CAT9K relay agent</td>
</tr>
<tr>
<td>CSCvk63089</td>
<td>show logging onboard switch active uptime detail shows 133 years as uptime</td>
</tr>
<tr>
<td>CSCvm00765</td>
<td>BFD crash on imitating traffic loss</td>
</tr>
<tr>
<td>CSCvm01064</td>
<td>PE stops VPLS traffic forwarding after xconnect flap</td>
</tr>
<tr>
<td>CSCvm33622</td>
<td>WCCP redirection to proxy server breaks in certain scenarios.</td>
</tr>
<tr>
<td>CSCvm35904</td>
<td>16.6.3: Access Tunnel Create Interface code is considered to be update request in FMAN_FP</td>
</tr>
<tr>
<td>CSCvm36333</td>
<td>MAC address programming issue</td>
</tr>
<tr>
<td>CSCvm39894</td>
<td>False authorizations and authentications even without radius server for dot1x/mab</td>
</tr>
<tr>
<td>CSCvm43071</td>
<td>[IBNS 2.0] aaa-available event is not being triggered when using authentication/authorization list</td>
</tr>
<tr>
<td>CSCvm43200</td>
<td>Traffic is not forward out on standby switch over SVL after SSO</td>
</tr>
<tr>
<td>CSCvm46814</td>
<td>session management process smd crash at cts_sga due to TDL memory depletion.</td>
</tr>
<tr>
<td>CSCvm60720</td>
<td>Broadcast Gratuitous ARP changed to unicast by switch leading to DHCP decline from client</td>
</tr>
<tr>
<td>CSCvm62274</td>
<td>Multicast traffic is software switched when switch is provisioned as Edge in Fabric - SDA Deployment</td>
</tr>
<tr>
<td>CSCvm63651</td>
<td>Memory leak due to authentication mac-move permit</td>
</tr>
<tr>
<td>CSCvm75378</td>
<td>Cat9x00: IPv6 SPAN filter still applied in hardware when removing entire monitor session</td>
</tr>
<tr>
<td>CSCvm81361</td>
<td>3850 stack SVL link status incorrect</td>
</tr>
<tr>
<td>CSCvm86135</td>
<td>SMD crash after removing access-session attributes filter-list</td>
</tr>
<tr>
<td>CSCvm89005</td>
<td>Packets looped internally during VXLAN decap in SD-Access environment</td>
</tr>
<tr>
<td>CSCvm93535</td>
<td>uRPF TCAM Resources exhausted even without uRPF configured on the switch</td>
</tr>
<tr>
<td>CSCvm97660</td>
<td>C9300 reflects back traffic on the same interface</td>
</tr>
<tr>
<td>CSCvm08672</td>
<td>DHCP packets cause unknown protocol drops on 16.6.x</td>
</tr>
<tr>
<td>CSCvn3698</td>
<td>WCCP Access-list might not be removed from interface after a WCCP loss of service</td>
</tr>
<tr>
<td>CSCvn46171</td>
<td>Rapid Memory Leak in &quot;FED Main Event&quot; Process due to Modifying Adjacencies</td>
</tr>
</tbody>
</table>
Resolved Caveats in Cisco IOS XE Everest 16.6.4a

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvj83551</td>
<td>SISF crash in IPV6 neighbor discovery packets</td>
</tr>
<tr>
<td>CSCvm36748</td>
<td>FED crash at expired &quot;FED MAC AGING TIMER&quot; or &quot;unknown&quot; timer without a stack trace.</td>
</tr>
<tr>
<td>CSCvm35904</td>
<td>16.6.3: Access Tunnel Create Interface code is considered to be update request in FMAN_FP</td>
</tr>
<tr>
<td>CSCvk60752</td>
<td>DHCP offer with Option 82 but no Remote ID suboption dropped by CAT9K relay agent</td>
</tr>
<tr>
<td>CSCvk32774</td>
<td>ACE entry with *established or range * in ACL drops TCP/UDP packets.</td>
</tr>
<tr>
<td>CSCvk31115</td>
<td>Device-sensor doesn't send data off initial boot</td>
</tr>
<tr>
<td>CSCvj86644</td>
<td>SDA: DHCP does not remove option 82 when sending packets to end-hosts</td>
</tr>
<tr>
<td>CSCvk39041</td>
<td>SDA: IP phone latency in fabric is close to 4 sec's</td>
</tr>
<tr>
<td>CSCvk02589</td>
<td>Connectivity is lost every four hours when ipv4 and ipv6 dual stack is configured.</td>
</tr>
<tr>
<td>CSCvk22204</td>
<td>stackwise virtual will blackhole traffic on standby unit after switchover, NIF is stuck</td>
</tr>
<tr>
<td>CSCvm09611</td>
<td>C9x00 crashed with multicast memory corruption.</td>
</tr>
<tr>
<td>CSCvj33865</td>
<td>Clearing mac address table should not delete entries created by control plane/remote entries</td>
</tr>
<tr>
<td>CSCvk07070</td>
<td>Observing bmalloc smd leaks at OBJ_WEBAUTH_LOGOUT_URL with webauth</td>
</tr>
<tr>
<td>CSCvk16813</td>
<td>DHCP client traffic dropped with DHCP snooping and port-channel or cross stack uplinks.</td>
</tr>
<tr>
<td>CSCvk46664</td>
<td>DNA Center SWIM Upgrade fails and unable to upgrade manually</td>
</tr>
<tr>
<td>CSCvk50734</td>
<td>Device Tracking - Memory leak observed with IPv6 NS/NA Packets</td>
</tr>
<tr>
<td>CSCvk53444</td>
<td>Packets with Fragment Offset not forwarded with DHCP Snooping Enabled in 16.6.4</td>
</tr>
<tr>
<td>CSCvm01064</td>
<td>PE stops VPLS traffic forwarding after xconnect flap</td>
</tr>
<tr>
<td>CSCvm09121</td>
<td>Evaluation of IOS-XE for CVE-2018-5391 (FragmentSmack)</td>
</tr>
</tbody>
</table>

Resolved Caveats in Cisco IOS XE Everest 16.6.4

The following are the resolved caveats in Cisco IOS XE Everest 16.6.4.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvk00115</td>
<td>Uplink FRU module hardware authentication failed</td>
</tr>
<tr>
<td>CSCvi69699</td>
<td>9400 - 9300: 40G copper QSFP interoperability broken (link down)</td>
</tr>
<tr>
<td>CSCvi83373</td>
<td>Repetitive logs show up 47K times in fed tracelogs</td>
</tr>
<tr>
<td>CSCvj52681</td>
<td>dynamic vlan assignment causes all sisf entries under the port to be deleted</td>
</tr>
<tr>
<td>CSCvi91714</td>
<td>IPv6 address not assigned or delayed when RA Guard is enabled</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCvi76084</td>
<td>Device-tracking entry stuck in TENTATIVE for certain Mac Pro hosts configured with static IP</td>
</tr>
<tr>
<td>CSCvi38916</td>
<td>Persistent Telnet and SSH crashes when configured in 16.6.2</td>
</tr>
<tr>
<td>CSCvi26398</td>
<td>&quot;%LISP-4-LOCAL_EID_RLOC_INCONSISTENCY&quot; should be supporessed in SDA context</td>
</tr>
<tr>
<td>CSCvi20882</td>
<td>Netconf IP-SLA udp-jitter case missing leaf codec</td>
</tr>
<tr>
<td>CSCvi11970</td>
<td>Abnormal output for show pnp tech-support</td>
</tr>
<tr>
<td>CSCvh85772</td>
<td>Switch not responding to ARP request for GW Anycast IP</td>
</tr>
<tr>
<td>CSCvh79942</td>
<td>Chunk corruption crash related to PNP or Guestshell</td>
</tr>
<tr>
<td>CSCvh21909</td>
<td>LISP: Overlapping prefix causes &quot;probe-down&quot; for map-cache entry</td>
</tr>
<tr>
<td>CSCvh09334</td>
<td>SDA-IPV6::SISF traceback @ar_relay_create_entry - L2 Binding tbl entry insertion failed</td>
</tr>
<tr>
<td>CSCvg45950</td>
<td>packet drop seen intermittently if 40G traffic sent via cts interface</td>
</tr>
<tr>
<td>CSCvb69966</td>
<td>Memory leak under LLDP Protocol process</td>
</tr>
<tr>
<td>CSCvg41950</td>
<td>Cisco IOS XE Software Diagnostic Shell Path Traversal Vulnerability</td>
</tr>
<tr>
<td>CSCvg53159</td>
<td>%SNMP-3-RESPONSE_DELAYED: processing GetNext of cafSessionEntry.2 seen on catalyst switch</td>
</tr>
<tr>
<td>CSCvg95580</td>
<td>interface speed config went lost after same FRU OIR with &quot;write mem&quot;</td>
</tr>
<tr>
<td>CSCvh48397</td>
<td>create_directory_cache: failed to stat flash message see when device managed by dnac</td>
</tr>
<tr>
<td>CSCvh66763</td>
<td>crash is seen at fed_l3_aal_delete_adj</td>
</tr>
<tr>
<td>CSCvh71539</td>
<td>Command &quot;show aaa servers&quot; reloads the switch</td>
</tr>
<tr>
<td>CSCvh84345</td>
<td>IOS CLI &quot;show platform software fed switch active punt cause summary&quot; may display negative counts</td>
</tr>
<tr>
<td>CSCvh87131</td>
<td>TRACEBACK: OID cefcModuleEntry crashes the box</td>
</tr>
<tr>
<td>CSCvh87270</td>
<td>StackWise Virtual not forwarding IGMP traffic over the standby switch.</td>
</tr>
<tr>
<td>CSCvi08459</td>
<td>set different words for username and password, but username shown the same as password</td>
</tr>
<tr>
<td>CSCvi09054</td>
<td>Stackwise Virtual: Routing Neighborships on Standby dont come up with MTU &gt; 9116</td>
</tr>
<tr>
<td>CSCvi19809</td>
<td>Memory leak in TMS process</td>
</tr>
<tr>
<td>CSCvi38191</td>
<td>Memory leak in Iman process due to &quot;ld_license_ext.dat&quot; build-up.</td>
</tr>
<tr>
<td>CSCvi39202</td>
<td>DHCP fails when DHCP snooping trust is enabled on uplink etherchannel</td>
</tr>
<tr>
<td>CSCvi70528</td>
<td>Cat9K- 40G QSFP Tx/Rx power out of valid range</td>
</tr>
<tr>
<td>CSCvi87106</td>
<td>Cat9K - 40G QSA adaptor, Rx power invalid.</td>
</tr>
<tr>
<td>CSCvi93137</td>
<td>Voice domain not forwarding for certain clients</td>
</tr>
<tr>
<td>CSCvj49476</td>
<td>Telnet Sessions Hang/Become unavailable at execution of &quot;show run&quot;</td>
</tr>
</tbody>
</table>
Resolved Caveats in Cisco IOS XE Everest 16.6.3

The following are the resolved caveats in Cisco IOS XE Everest 16.6.3:

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvh31431</td>
<td>Memory leak in linux_iosd-image on 16.6 releases.</td>
</tr>
<tr>
<td>CSCvh52882</td>
<td>Memory Leak due to nbar config.</td>
</tr>
<tr>
<td>CSCvh69402</td>
<td>Dot1x specific configuration applied but not working on the interface.</td>
</tr>
<tr>
<td>CSCvh81152</td>
<td>Local SVI IP is registered as dynamic-eid.</td>
</tr>
<tr>
<td>CSCvh06383</td>
<td>16.6.x: Intermittent traffic loss for MAB devices after successful initial authentication.</td>
</tr>
<tr>
<td>CSCvg58682</td>
<td>Stackwise SNMP OID for cswDistrStackPhyPort and cswDistrStackPhyPortNbr not working.</td>
</tr>
<tr>
<td>CSCvg56727</td>
<td>Crashes with 'server-key' command using key of 128 characters or more.</td>
</tr>
<tr>
<td>CSCve32330</td>
<td>%UTIL-6-RANDOM: A pseudo-random number was generated twice in succession.</td>
</tr>
<tr>
<td>CSCvg22515</td>
<td>After upgrade of IOS, SSH passwords longer than 25 characters do not work.</td>
</tr>
<tr>
<td>CSCvg60288</td>
<td>Device IP address AV pair replaced with 192.168.1.5.</td>
</tr>
<tr>
<td>CSCvh32416</td>
<td>Evaluation of all for CPU Side-Channel Information Disclosure Vulnerability.</td>
</tr>
<tr>
<td>CSCvh55578</td>
<td>To add recovery mechanism for glean entry.</td>
</tr>
<tr>
<td>CSCvf84349</td>
<td>Router crash on polling cEigrpPeerEntry.</td>
</tr>
</tbody>
</table>

Resolved Caveats in Cisco IOS XE Everest 16.6.2

The following are the resolved caveats in Cisco IOS XE Everest 16.6.2.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvf36657</td>
<td>Catalyst 9500: Interface not coming up after shut/no-shut.</td>
</tr>
<tr>
<td>CSCvf75518</td>
<td>Controller port error interface.</td>
</tr>
</tbody>
</table>

Resolved Caveats in Cisco IOS XE Everest 16.6.1

The following are the resolved caveats in Cisco IOS XE Everest 16.6.1.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCve29216</td>
<td>9500-WebUI: Upon hovering an interface, status description is incorrectly displayed as no link</td>
</tr>
</tbody>
</table>

Troubleshooting

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

Choose **Product Support > WirelessSwitches**. Then choose your product and click **Troubleshoot and Alerts** to find information for the problem that you are experiencing.

**Related Documentation**

- Cisco Catalyst 9500 Series Switches documentation at this URL:  
  http://www.cisco.com/go/c9500
- Cisco IOS XE 16 documentation at this URL:  
- Cisco SFP and SFP+ modules documentation, including compatibility matrices at this URL:  
- Cisco Validated Designs documents at this URL:  
  http://www.cisco.com/go/designzone
Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the *What’s New in Cisco Product Documentation*, which lists all new and revised Cisco Technical documentation, as an RSS feed and deliver content directly to your desktop using a read application. The RSS feeds are a free service.

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: www.cisco.com/go/trademarks. 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)

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.

© 2019 Cisco Systems, Inc. All rights reserved.