



# Release Notes for the Catalyst 4500E Series Switch, Cisco IOS XE Release 3.8.xE

---

**First Published: October 1, 2015**

**Last Updated: Sep 24, 2019**

This release note describes the features, modifications, and caveats for the Cisco IOS XE Release 3.8.xE software on the Catalyst 4500E series switch with Supervisor Engine 7-E, 7L-E, 8-E, and 8L-E.



**Note**

---

Beginning with Cisco IOS XE Release 3.8.1E, Supervisor Engine 8L-E is available with ROMMON 15.1(1r)SG6

---



**Note**

---

For the Supervisor Engine 8-E to support Cisco IOS XE Release 3.8.xE, the ROMMON version must be upgraded to 15.1(1r)SG5. (Refer to "[Upgrading the System Software](#)" 48).

---

Cisco IOS XE Release 3.8.xE is a feature rich new software feature release for IOS and IOS-XE based Catalyst Access Switching products. This release will provide extended maintenance.

Support for Cisco IOS XE Release 3.8.xE follows the standard Cisco Systems® support policy, available at

[http://www.cisco.com/en/US/products/products\\_end-of-life\\_policy.html](http://www.cisco.com/en/US/products/products_end-of-life_policy.html)

For more information on the Catalyst 4500E series switches, visit the following URL:

<http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html>



**Note**

---

Although this release note and those for the Catalyst 4900M, Catalyst 4948E, Catalyst 4948E-F Series Switches, Catalyst 4500 Series Switches, and the Catalyst 4500-X Series Switches differ, each leverages the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide*.

---



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Contents

This publication consists of these sections:

- [Cisco IOS Software Packaging](#)
- [Cisco XE Release Strategy](#)
- [System Requirements](#)
- [New and Changed Information](#)
- [Cisco IOS XE to Cisco IOS](#)
- [Wireless Related Information](#)
- [Upgrading the System Software](#)
- [Limitations and Restrictions](#)
- [Caveats](#)
- [Related Documentation](#)
- [Notices](#)

## Cisco IOS Software Packaging

The Enterprise Services image supports all Cisco Catalyst 4500E Series software features based on Cisco IOS Software, including enhanced routing.

The IP Base image supports Open Shortest Path First (OSPF) for Routed Access, Enhanced Interior Gateway Routing Protocol (EIGRP) "limited" Stub Routing, Nonstop Forwarding/Stateful Switchover (NSF/SSO), and RIPv1/v2. The IP Base image does not support enhanced routing features such as BGP, Intermediate System-to-Intermediate System (IS-IS), Full OSPF, Full Enhanced Interior Gateway Routing Protocol (EIGRP) & Virtual Routing Forwarding (VRF-lite).

The LAN Base image complements the existing IP Base and Enterprise Services images. It is focused on customer access and Layer 2 requirements and therefore many of the IP Base features are not required.

Starting with Cisco IOS Release XE 3.5.0E, OSPF Routed Access in IP Base support rose to 1000 routes.

## Cisco XE Release Strategy

Customers with Catalyst 4500 Series Switches who need the latest hardware and software features should migrate to Cisco IOS XE Release 3.8.xE.

IOS XE 3.2.xSG is an active maintenance train that supports Sup7E only.

IOS XE 3.4.xSG is a maintenance train supporting Sup7E and Sup7L-E.

IOS XE 3.6.xSG is a maintenance train supporting Sup7E, Sup7L-E and Sup8-E.

IOS XE 3.8.xE is a maintenance train supporting Sup7E, Sup7L-E and Sup8-E.

IOS XE 3.8.1E and later supports Sup8L-E.

IOS XE 3.8.xE, 3.6.xE, 3.4.xSG, and 3.2.xSG are extended maintenance (EM) releases.

IOS XE 3.7.xE, 3.5.xE, and 3.3.0SG are standard releases (SM).

## Support

Support for Cisco IOS XE Release 3.8.xE follows the standard Cisco Systems® support policy, available at

[http://www.cisco.com/en/US/products/products\\_end-of-life\\_policy.html](http://www.cisco.com/en/US/products/products_end-of-life_policy.html)

## System Requirements

This section describes the system requirements:

- [Supported Hardware on the Catalyst 4500E Series Switch](#)
- [Supported E-Series Hardware on Cisco IOS XE Release 3.8.xE](#)
- [Feature Support by Image Type](#)
- [OpenFlow Version and Cisco IOS Release Support](#)
- [MIB Support](#)
- [Features Not Supported on the Cisco Catalyst 4500-E Series Switch](#)
- [Orderable Product Numbers](#)



### Note

For information about wireless web UI requirements, see “[Wireless Web UI Software Requirements](#)” section on page 42

## Supported Hardware on the Catalyst 4500E Series Switch

- [Table 1 Supported Hardware on Cisco Catalyst 4500E, 3](#)
- [Table 2 Supported Pluggable Transceiver Modules, 6](#)
- [Table 3 Power over Ethernet on Cisco Catalyst 4500-E, 7](#)

**Table 1** Supported Hardware on Cisco Catalyst 4500E

Product Number (append with “=” for spares)	Product Description
<b>Supervisor Engines</b>	
WS-X45-Sup7-E	Catalyst 4500-E series switch Supervisor Engine 7-E <b>Note</b> This engine is supported on E-series, R-E, and R+E chassis.
WS-X45-Sup7L-E	Catalyst 4500-E series switch Supervisor Engine 7L-E <b>Note</b> This engine is supported on E-series, R-E, and R+E chassis.
WS-X45-Sup8-E	Catalyst 4500-E series switch Supervisor Engine 8-E This engine is supported on E-series and R+E and R-E <sup>1</sup> chassis.
WS-X45-Sup8L-E	Catalyst 4500-E series switch Supervisor Engine 8L-E This engine is supported on E-series and R+E and R-E <sup>1</sup> chassis.

**Table 1 Supported Hardware on Cisco Catalyst 4500E**

Product Number (append with “=” for spares)	Product Description
<b>10 Gigabit Ethernet Switching Modules</b>	
WS-X4748-12X48U+E	Catalyst 4500E 48-Port UPOE with 12 Multigigabit ports and 36 10/100/1000 ports. This module supports the Cisco Multigigabit technology for 802.11ac Wave2 and 10GBASE-T speeds.
WS-X4712-SFP+E	12-port 10 Gigabit Ethernet (SFP+) line card Not supported on 4507R-E and 4510R-E chassis.
WS-X4606-X2-E	6-port X2 line card
<b>Gigabit Ethernet Switching Modules</b>	
WS-X4302-GB	2-port 1000BASE-X (GBIC) Gigabit Ethernet module. Not supported in VSS mode.
WS-X4306-GB	6-port 1000BASE-X (GBIC) Gigabit Ethernet switching module
WS-X4418-GB	18-port 1000BASE-X (GBIC) Gigabit Ethernet switching module. Not supported in VSS mode.
WS-X4412-2GB-T	12-port 1000BASE-T Gigabit Ethernet and 2-GBIC ports switching module. Not supported in VSS mode.
WS-X4424-GB-RJ45	24-port 10/100/1000BASE-T Gigabit Ethernet RJ-45 switching module Not supported in VSS mode.
WS-X4448-GB-LX	48-port 1000BASE-LX (small form-factor pluggable) Gigabit Ethernet fiber optic interface switching module. Not supported in VSS mode.
WS-X4448-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet switching module. Not supported in VSS mode.
WS-X4448-GB-SFP	48-port 1000BASE-X (small form-factor pluggable) module. Not supported in VSS mode.
WS-X4506-GB-T	6-port Alternately-Wired 10/100/1000BASE-T Catalyst 4500 series Power over Ethernet (PoE) 802.3af or 1000BASE-X SFP. Not supported in VSS mode.
WS-X4524-GB-RJ45V	24-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af. Not supported in VSS mode.
WS-X4548-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet module. Not supported in VSS mode.
WS-X4548-GB-RJ45V	48-port 10/100/1000BASE-T, Gigabit Ethernet module with PoE IEEE 802.3af. This module is supported on Supervisor Engines 7E and 7LE, but not on Supervisor Engines 8E and 8LE. This module is not supported in VSS mode.

**Table 1** Supported Hardware on Cisco Catalyst 4500E

<b>Product Number</b> (append with "=" for spares)	<b>Product Description</b>
WS-X4548-RJ45V+	48-port 10/100/1000BASE-T, Gigabit Ethernet module with IEEE 802.3af PoEP and IEEE 802.3at PoEP. This module is supported on Supervisor Engines 7-E and 7L-E, but not on Supervisor Engines 8-E and 8L-E.
WS-X4612-SFP-E	12-port 1000BASE-X (small form factor pluggable) module with jumbo frame support
WS-X4624-SFP-E	Non-blocking 24-port 1000BASEX (small form factor pluggable) module
WS-X4640-CSFP-E	80 ports with Gigabit compact SFP (4:1 oversubscribed); 40 modules of Gigabit SFP line card (1000BaseX), providing 24 gigabits per-slot capacity (SFP optional) (2:1 oversubscribed)
WS-X4648-RJ45-E	48 port 10/100/1000BT with 2 to 1 oversubscription and jumbo frame support
WS-X4648-RJ45V-E	48 port 10/100/1000 Mb with 2 to 1 oversubscription PoE 802.3af providing up to 20 Watts power/port
WS-X4648-RJ45V+E	48 port 10/100/1000 Mb with 2 to 1 oversubscription PoE 802.3at providing up to 30 Watts power/port
WS-X4748-RJ45V+E	48-port 10/100/1000 line card nonblocking PoE 802.3at providing up to 30 Watts power/port
WS-X4748-UPOE+E	48-port 10/100/1000 line card nonblocking PoE 802.3at and 60 watt UPoE PoE linecard with Ethernet Energy Efficient feature.
WS-X4748-RJ45-E	48-port 10/100/1000 nonblocking line card with the Ethernet Energy Efficient feature
WS-X4748-SFP-E	48-port 1000Base-X SFP (small form factor pluggable) line card
WS-X4724-SFP-E	24-port 1000Base-X SFP (small form factor pluggable) line card
WS-X4712-SFP-E	12-port 1000Base-X SFP (small form factor pluggable) line card
<b>Fast Ethernet Switching Modules</b>	
WS-X4124-FX-MT	24-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module. Not supported in VSS mode.
WS-X4148-FX-MT	48-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module
WS-X4148-FE-LX-MT	48-port 100BASE-LX10 Fast Ethernet MT-RJ single-mode fiber switching module. Not supported in VSS mode.
WS-X4148-FE-BD-LC	48-port 100BASE-BX10-D module
WS-X4248-FE-SFP	48-port 100BASE-X SFP switching module
WS-U4504-FX-MT	4-port 100BASE-FX (MT-RF) uplink daughter card
WS-X4504-FX-MT	4-port 100BASE-FX MT-RJ uplink module. Not supported in VSS mode.
<b>Ethernet/Fast Ethernet (10/100) Switching Modules</b>	
WS-X4124-RJ45	24-port 10/100 RJ-45 module. Not supported in VSS mode.
WS-X4148-RJ	48-port 10/100 RJ-45 switching module
WS-X4148-RJ21	48-port 10/100 4xRJ-21 (telco connector) switching module. Not supported in VSS mode.

**Table 1 Supported Hardware on Cisco Catalyst 4500E**

<b>Product Number</b> (append with “=” for spares)	<b>Product Description</b>
WS-X4148-RJ45V	48-port Pre-standard PoE 10/100BASE-T switching module. Not supported in VSS mode.
WS-X4224-RJ45V	24-port 10/100BASE-TX RJ-45 Cisco Catalyst 4500 series PoE 802.3af. Not supported in VSS mode.
WS-X4232-GB-RJ	32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet switching module. Not supported in VSS mode.
WS-X4248-RJ21V	48-port 10/100 Fast Ethernet RJ-21 Cisco Catalyst 4500 series PoE 802.3af telco. Not supported in VSS mode.
WS-X4248-RJ45V	48-port 10/100 Fast Ethernet RJ-45 Cisco Catalyst 4500 series PoE 802.3af. This module is supported only on Supervisor Engines 7-E and 7L-E, but not supported on Supervisor Engines 8-E and 8L-E.
WS-X4232-RJ-XX	32-port 10/100 Fast Ethernet RJ-45 modular uplink switching module. Not supported in VSS mode.
WS-X4232-L3	32-port 10/100 Fast Ethernet, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet services module. Not supported in VSS mode.
<b>Other Modules</b>	
MEM-X45-2GB-E	SD Card, 2G
USB-X45-4GB-E	USB Thumb Drive, 4G
<b>Product Number</b> (append with “=” for spares)	<b>Product Description</b>

1. To support Supervisor Engine 8-E or 8L-E, the Cisco Catalyst 4507R-E Switch chassis must have hardware revision 2.0 or higher. For information about identifying the revision numbers see the [“Identifying Hardware Revisions on the Switch Chassis”](#) section on page 49.

**Table 2 Supported Pluggable Transceiver Modules**

<b>Module Type</b>	<b>URL</b>
Cisco 10-Gigabit Ethernet Transceiver Modules Compatibility Matrix	<a href="http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/10GE_Tx_Matrix.html">http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/10GE_Tx_Matrix.html</a>
Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix	<a href="http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/GE_Tx_Matrix.html">http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/GE_Tx_Matrix.html</a>
Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix	<a href="http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/100MB_Tx_Matrix.html">http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/100MB_Tx_Matrix.html</a>

**Table 2** Supported Pluggable Transceiver Modules

Module Type	URL
Cisco Wavelength Division Multiplexing Transceivers Compatibility Matrix	<a href="http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6982.html">http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6982.html</a>
Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix	<a href="http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/40GE_Tx_Matrix.html">http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/40GE_Tx_Matrix.html</a>

**Table 3** Power over Ethernet on Cisco Catalyst 4500-E

Type	URL
Power over Ethernet on the Cisco Catalyst 4500E Series Platform Data Sheet	<a href="http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/product_data_sheet09186a00801f3dd9.html">http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/product_data_sheet09186a00801f3dd9.html</a>

## Supported E-Series Hardware on Cisco IOS XE Release 3.8.xE

A brief list of primary E-Series hardware supported by Cisco IOS XE Release 3.8.xE is shown in [Table 4](#).

**Table 4** Supported E-Series Hardware

Product Number	Description
WS-C4503-E	Cisco Catalyst 4500-E Series 3-Slot Chassis <ul style="list-style-type: none"> <li>Fan tray</li> <li>No Power Supply</li> </ul>
WS-C4506-E	Cisco Catalyst 4500-E Series 6-Slot Chassis <ul style="list-style-type: none"> <li>Fan tray</li> <li>No Power Supply</li> </ul>
WS-C4507R-E	Cisco Catalyst 4500-E Series 7-Slot Chassis <ul style="list-style-type: none"> <li>Fan tray</li> <li>No Power Supply</li> <li>Redundant supervisor engine capability</li> <li>In this chassis, supervisor engines must sit in slots 3 and/or 4; the backplane will enforce this restriction.</li> </ul> <p><b>Note</b> The WS-C4507R-E module requires hardware revision 2.0 or higher to support Supervisor Engines 8-E and 8L-E.</p>
WS-C4507R+E	Cisco Catalyst 4500-E Series 7-Slot 48 GB-ready Chassis <ul style="list-style-type: none"> <li>Fan tray</li> <li>No Power Supply</li> <li>Redundant supervisor engine capability</li> <li>In this chassis, supervisor engines must sit in slots 3 and/or 4; the backplane will enforce this restriction.</li> </ul>

**Table 4 Supported E-Series Hardware**

Product Number	Description
WS-C4510R-E	<p>Cisco Catalyst 4500-E Series 10-Slot Chassis</p> <p><b>Note</b> This chassis does not support Supervisor Engines 7L-E and 8L-E.</p> <ul style="list-style-type: none"> <li>• Fan tray</li> <li>• No Power Supply</li> <li>• Redundant supervisor engine capability</li> <li>• In this chassis, supervisor engines must sit in slots 5 and/or 6; the backplane will enforce this restriction.</li> </ul>
WS-C4510R+E	<p>Cisco Catalyst 4500-E Series 10-Slot 48 GB-ready Chassis</p> <p><b>Note</b> This chassis does not support Supervisor Engines 7L-E and 8L-E.</p> <ul style="list-style-type: none"> <li>• Fan tray</li> <li>• No Power Supply</li> <li>• Redundant supervisor engine capability</li> <li>• In this chassis, supervisor engines must sit in slots 5 and/or 6; the backplane will enforce this restriction.</li> </ul>

## Wired Web UI (Device Manager) System Requirements

### Software Requirements

- Windows 2000, Windows 2003, Windows XP, Windows Vista, or Windows 7
- With JavaScript enabled: Internet Explorer 6.0 and 7.0, or Firefox 26.0

## Feature Support by Image Type

Table 5 is a detailed list of features supported on Catalyst 4500-E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E running Cisco IOS XE Release 3.8.xE categorized by image type. Please visit Feature Navigator for package details:

<http://tools.cisco.com/ITDIT/CFN/>



### Note

Wireless features supported on Supervisor Engine 8-E are available only on IP Base and Enterprise Services images.

**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
2-way Community Private VLANs	Yes	Yes	Yes



**Table 5** LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E

Feature	LAN Base	IP Base	Enterprise Services
8-Way CEF Load Balancing	Yes	Yes	Yes
10 Gigabit Uplink Use	Yes	Yes	Yes
AAA Server Group	Yes	Yes	Yes
AAA Server Group Based on DNIS	Yes	Yes	Yes
ACL - Improved Merging Algorithm	Yes	Yes	Yes
ACL Logging	Yes	Yes	Yes
ACL Policy Enhancements	Yes	Yes	Yes
ACL Sequence Numbering	Yes	Yes	Yes
Address Resolution Protocol (ARP)	Yes	Yes	Yes
ANCP Client	No	Yes	Yes
ANSI TIA-1057 LLDP - MED Location Extension	Yes	Yes	Yes
ANSI TIA-1057 LLDP - MED Support	Yes	Yes	Yes
ARP Optimization	Yes	Yes	Yes
Auto Configuration	Yes	Yes	Yes
Auto Identity	No	Yes	Yes
Auto-LAG	Yes	Yes	Yes
Auto QoS	Yes	Yes	Yes
Auto QoS Compact	Yes	Yes	Yes
Auto Security	Yes	Yes	Yes
Auto SmartPorts	Yes	Yes	Yes
Auto-MDIX	Yes	Yes	Yes
Auto-Voice VLAN (part of Auto QoS)	Yes	Yes	Yes
AutoInstall Using DHCP for LAN Interfaces	Yes	Yes	Yes
AutoQoS - VoIP	Yes	Yes	Yes
AutoRP Enhancement	No	Yes	Yes

**Table 5** LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E

Feature	LAN Base	IP Base	Enterprise Services
Banner Page and Inactivity timeout for HTTP/S connections	Yes	Yes	Yes
BGP	No	No	Yes
BGP 4	No	No	Yes
BGP 4 4Byte ASN (CnH)	No	No	Yes
BGP 4 Multipath Support	No	No	Yes
BGP 4 Prefix Filter and In-bound Route Maps	No	No	Yes
BGP 4 Soft Config	No	No	Yes
BGP Conditional Route Injection	No	No	Yes
BGP Configuration Using Peer Templates	No	No	Yes
BGP Dynamic Update Peer-Groups	No	No	Yes
BGP Increased Support of Numbered as-path Access Lists to 500	No	No	Yes
BGP Link Bandwidth	No	No	Yes
BGP Neighbor Policy	No	No	Yes
BGP Prefix-Based Outbound Route Filtering	No	No	Yes
BGP Restart Neighbor Session After max-prefix Limit Reached	No	No	Yes
BGP Route-Map Continue	No	No	Yes
BGP Route-Map Continue Support for Outbound Policy	No	No	Yes
BGP Soft Rest	No	No	Yes
BGP Wildcard	No	No	Yes
Bidirectional PIM (IPv4 only)	No	Yes	Yes
Bidirectional SXP support	Yes	Yes	Yes
Bidirectional Forwarding Detection (BFD) for Intermediate System to Intermediate System (IS-IS)	No	No	Yes
Boot Config	Yes	Yes	Yes
Broadcast/Multicast Suppression	Yes	Yes	Yes

**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
Call Home	No	Yes	Yes
CDP (Cisco Discovery Protocol) Version 2	Yes	Yes	Yes
CDP Enhancement - Host presence TLV	Yes	Yes	Yes
CEF/dCEF - Cisco Express Forwarding	Yes	Yes	Yes
CEFv6 Switching for 6to4 Tunnels	No	Yes	Yes
CEFv6/dCEFv6 - Cisco Express Forwarding	Yes	Yes	Yes
CFM/IEEE 802.1ag - D8.1 standard Compliant CFM, Y.1731 multicast LBM / AIS / RDI / LCK, IP SLA for Ethernet	Yes	Yes	Yes
CGMP - Cisco Group Management Protocol	No	Yes	Yes
Cisco IOS Scripting w/Tcl	Yes	Yes	Yes
Cisco Plug-in for OpenFlow	Yes	Yes	Yes
Cisco Service Discovery Gateway Support	Yes	Yes	Yes
Cisco TrustSec—IEEE 802.1ae MACSec Layer 2 encryption	No	Yes	Yes
Cisco TrustSec—IEEE 802.1ae MACSec encryption on user facing ports	No	Yes	Yes
Cisco TrustSec—IEEE 802.1ae MACSec encryption on user facing ports SSO	No	Yes	Yes
Cisco TrustSec—IEEE 802.1ae MACSec encryption between switch-to-switch links using Cisco SAP (Security Association Protocol)	No	Yes	Yes
Cisco TrustSec—Critical Authentication	Yes	Yes	Yes
Cisco TrustSec—SGT Exchange Protocol (SXP) IPv4	No	Yes	Yes
Cisco TrustSec—SGT/ SGA	No	Yes	Yes
Cisco TrustSec—SGACL Logging and Statistics	No	Yes	Yes
CiscoView Autonomous Device Manager (ADP)	No	Yes	Yes
Class Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)	Yes	Yes	Yes

**Table 5** LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E

Feature	LAN Base	IP Base	Enterprise Services
Class-Based Marking	Yes	Yes	Yes
Class-Based Policing	Yes	Yes	Yes
Class-Based Shaping	Yes	Yes	Yes
Clear Counters Per Port	Yes	Yes	Yes
CLI String Search	Yes	Yes	Yes
CNS	Yes	Yes	Yes
CNS - Configuration Agent	Yes	Yes	Yes
CNS - Event Agent	Yes	Yes	Yes
CNS - Image Agent	Yes	Yes	Yes
CNS - Interactive CLI	Yes	Yes	Yes
CNS Config Retrieve Enhancement with Retry and Interval	Yes	Yes	Yes
Command Scheduler (Kron)	Yes	Yes	Yes
Command Scheduler (Kron) Policy for System Startup	Yes	Yes	Yes
Commented IP Access List Entries	Yes	Yes	Yes
Community Private VLAN	Yes	Yes	Yes
Configuration Change Tracking Identifier	Yes	Yes	Yes
Configuration Change Notification and Logging	No	Yes	Yes
Configuration Replace and Configuration Rollback	Yes	Yes	Yes
Configuration Rollback Confirmed Change	Yes	Yes	Yes
Configuring FQDN ACL	Yes	Yes	Yes
Contextual Configuration Diff Utility	Yes	Yes	Yes
Control Plane Policing (Copp)	Yes	Yes	Yes
Control Plane Protection (Wireless)	No	Yes	Yes
CPU Optimization for Layer 3 Multicast Control Packets	Yes	Yes	Yes
Critical Authorization for Voice and Data	Yes	Yes	Yes
DAI (Dynamic ARP inspection)	Yes	Yes	Yes

**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
DBL (Dynamic Buffer Limiting) - Selective DBL	Yes	Yes	Yes
Debounce Timer per Port	Yes	Yes	Yes
Default Passive Interface	No	Yes	Yes
DHCP Client	Yes	Yes	Yes
DHCP Configurable DHCP Client	Yes	Yes	Yes
DHCP Gleaning	No	Yes	Yes
DHCPv6 Relay Agent notification for Prefix Delegation	Yes	Yes	Yes
DHCP Option 82, Pass Through	Yes	Yes	Yes
DHCP Server	Yes	Yes	Yes
DHCP Snooping	Yes	Yes	Yes
DHCPv6 Ethernet Remote ID option	Yes	Yes	Yes
DHCPv6 Relay - Reload persistent Interface ID option	Yes	Yes	Yes
DHCPv6 Repackaging	Yes	Yes	Yes
Diffserv MIB	Yes	Yes	Yes
DSCP/CoS via LLDP	Yes	Yes	Yes
Duplication Location Reporting Issue	No	Yes	Yes
Dynamic Trunking Protocol (DTP)	Yes	Yes	Yes
Easy Virtual Network (EVN)	No	No	Yes
Easy VSS <sup>1</sup>	No	Yes (SUP7E and SUP8E only)	Yes (SUP7E, SUP7LE, and SUP8E, SUP8LE)
EIGRP	No	No	Yes
EIGRP Service Advertisement Framework	Yes	Yes	Yes
EIGRP Stub Routing	No	Yes	Yes
Embedded Event Manager (EEM) 3.2	No	Yes	Yes
Embedded Syslog Manager (ESM)	Yes	Yes	Yes

**Table 5** LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E

Feature	LAN Base	IP Base	Enterprise Services
Enable Bidirectional SXP support	Yes	Yes	Yes
Enable of Security Group ACL at Interface Level	Yes	Yes	Yes
Energywise Agentless SNMP support	Yes	Yes	Yes
Energywise Wake-On-Lan Support	Yes	Yes	Yes
Enhanced PoE Support (Additional Wattage Range)	Yes	Yes	Yes
Entity API for Physical and Logical Mgd Entities	Yes	Yes	Yes
ErrDisable timeout	Yes	Yes	Yes
EtherChannel	Yes	Yes	Yes
EtherChannel Flexible PAgP	Yes	Yes	Yes
EtherChannel Single Port Channel	Yes	Yes	Yes
Ethernet Virtual Connections (EVC)-Lite	No	Yes	Yes
Fast EtherChannel (FEC)	Yes	Yes	Yes
FHRP - Enhanced Object Tracking of IP SLAs	Yes	Yes	Yes
FHRP - Enhanced Object Tracking integration with EEM	Yes	Yes	Yes
FHRP - GLBP - IP Redundancy API	No	Yes	Yes
FHRP - HSRP - Hot Standby Router Protocol V2	No	Yes	Yes
FHRP - Object Tracking List	No	Yes	Yes
Filter-ID Based ACL Application	Yes	Yes	Yes
FIPS 140-2/3 Level 2 Certification	Yes	Yes	Yes
FIPS/CC Compliance for NMSP	Yes	Yes	Yes
Flexible NetFlow - Application ID	No	Yes	Yes
Flexible NetFlow - CTS Fields	No	Yes	Yes
Flexible NetFlow - Device type	No	Yes	Yes
Flexible NetFlow - Ethertype	No	Yes	Yes
Flexible NetFlow - Full Flow support	No	Yes	Yes
Flexible NetFlow - Ingress support	No	Yes	Yes

**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
Flexible NetFlow - IPv4 Unicast Flows	No	Yes	Yes
Flexible NetFlow - IPv6 Unicast Flows	No	Yes	Yes
Flexible NetFlow - Layer 2 Fields	No	Yes	Yes
Flexible NetFlow - Multiple User Defined Caches	No	Yes	Yes
Flexible NetFlow - NetFlow Export over IPv4	No	Yes	Yes
Flexible NetFlow - NetFlowV5 Export protocol	No	Yes	Yes
Flexible NetFlow - NetFlow v9 Export Format	No	Yes	Yes
Flexible NetFlow - Power Reading	No	Yes	Yes
Flexible NetFlow - Username	No	Yes	Yes
Flexible NetFlow - VLAN ID support	No	Yes	Yes
Flexible NetFlow - Export to an IPv6 address	No	Yes	Yes
Flexible NetFlow - IPFIX	No	Yes	Yes
Flex Links+(VLAN Load balancing)	Yes	Yes	Yes
Forced 10/100 Autonegotiation	Yes	Yes	Yes
FQDN	Yes	Yes	Yes
FTP Support for Downloading Software Images	Yes	Yes	Yes
Gateway Load Balancing Protocol (GLBP)	No	Yes	Yes
Generic Routing Encapsulation (GRE)	No	Yes	Yes
GOLD Online Diagnostics	Yes	Yes	Yes
GRE Tunneled Packets Switched on Hardware	No	No	Yes
HSRP: Global IPv6 Address	No	Yes	Yes
HSRP - Hot Standby Router Protocol	No	Yes	Yes
HSRPv2 for IPv6 Global Address Support	No	Yes	Yes
HTTP Gleaning	No	Yes	Yes
HTTP Security	Yes	Yes	Yes
HTTP TACAC+ Accounting support	Yes	Yes	Yes

**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
IEEE 802.1ab LLDP (Link Layer Discovery Protocol)	Yes	Yes	Yes
IEEE 802.1ab LLDP/LLDP-MED	Yes	Yes	Yes
IEEE 802.1ab LLDP enhancements (PoE+Layer 2 COS)	Yes	Yes	Yes
IEEE 802.1p Support	Yes	Yes	Yes
IEEE 802.1Q VLAN Trunking	Yes	Yes	Yes
IEEE 802.1s Multiple Spanning Tree (MST) Standard Compliance	Yes	Yes	Yes
IEEE 802.1s VLAN Multiple Spanning Trees	Yes	Yes	Yes
IEEE 802.1t <sup>2</sup>	Yes	Yes	Yes
IEEE 802.1w Spanning Tree Rapid Reconfiguration	Yes	Yes	Yes
IEEE 802.1x Auth Fail Open (Critical Ports)	Yes	Yes	Yes
IEEE 802.1x Auth Fail VLAN	Yes	Yes	Yes
IEEE 802.1x Flexible Authentication	Yes	Yes	Yes
IEEE 802.1x Multiple Authentication	Yes	Yes	Yes
IEEE 802.1x Open Authentication	Yes	Yes	Yes
IEEE 802.1X with User Distribution	Yes	Yes	Yes
IEEE 802.1x VLAN Assignment	Yes	Yes	Yes
IEEE 802.1x VLAN User Group Distribution	Yes	Yes	Yes
IEEE 802.1x Wake on LAN Support	Yes	Yes	Yes
IEEE 802.1x Authenticator	Yes	Yes	Yes
IEEE 802.1x Fallback support	Yes	Yes	Yes
IEEE 802.1x Guest VLAN	Yes	Yes	Yes
IEEE 802.1x Multi-Domain Authentication	Yes	Yes	Yes
IEEE 802.1x Private Guest VLAN	Yes	Yes	Yes
IEEE 802.1x Private VLAN Assignment	Yes	Yes	Yes
IEEE 802.1x RADIUS Accounting	Yes	Yes	Yes



**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
IEEE 802.1x RADIUS-Supplied Session Timeout	Yes	Yes	Yes
IEEE 802.1x with ACL Assignments	Yes	Yes	Yes
IEEE 802.1x with Port Security	Yes	Yes	Yes
IEEE 802.3ad Link Aggregation (LACP)	Yes	Yes	Yes
IEEE 802.3ad Link Aggregation (LACP) Port-Channel Standalone Disable	Yes	Yes	Yes
IEEE 802.3af PoE (Power over Ethernet)	Yes	Yes	Yes
IEEE 802.3x Flow Control	Yes	Yes	Yes
IGMP Fast Leave	Yes	Yes	Yes
IGMP Filtering	Yes	Yes	Yes
IGMP Snooping	Yes	Yes	Yes
IGMP Version 1	Yes	Yes	Yes
IGMP Version 2	Yes	Yes	Yes
IGMP Version 3	Yes	Yes	Yes
IGMP Version 3 - Explicit Tracking of Hosts, Groups, and Channels	Yes	Yes	Yes
IGMPv3 Host Stack	Yes	Yes	Yes
IGMPv3 Snooping: Full Support	Yes	Yes	Yes
Image Verification	Yes	Yes	Yes
Individual SNMP Trap Support	Yes	Yes	Yes
Inline Power Auto Negotiation	Yes	Yes	Yes
Inline Power Management	Yes	Yes	Yes
Interface Index Persistence	Yes	Yes	Yes
Interface Range Specification	Yes	Yes	Yes
Interface Templates	Yes	Yes	Yes
IOS Based Device Profiling	No	Yes	Yes
IP Enhanced IGRP Route Authentication	No	No	Yes

**Table 5** LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E

Feature	LAN Base	IP Base	Enterprise Services
IP Event Dampening	No	Yes	Yes
IP Multicast Load Splitting - Equal Cost Multipath (ECMP) using S, G and Next-hop	No	No	Yes
IP Multicast Load Splitting across Equal-Cost Paths	No	Yes	Yes
IP Named Access Control List	Yes	Yes	Yes
IPv6 Tunnels (in software)	No	Yes	Yes
IP Routing	Yes	Yes	Yes
IP SLAs - DHCP Operations	No	Yes	Yes
IP SLAs - Distribution of Statistics	No	Yes	Yes
IP SLAs - DNS Operation	No	Yes	Yes
IP SLAs - FTP Operation	No	Yes	Yes
IP SLA - HTTP Operation	No	Yes	Yes
IP SLAs - ICMP Echo Operation	No	Yes	Yes
IP SLAs - ICMP Path Echo Operation	No	Yes	Yes
IP SLAs - Multi Operation Scheduler	No	Yes	Yes
IP SLAs - One Way Measurement	No	Yes	Yes
IP SLAs - Path Jitter Operation	No	Yes	Yes
IP SLAs - Random Scheduler	No	Yes	Yes
IP SLAs - Reaction Threshold	No	Yes	Yes
IP SLAs - Responder	Yes	Yes	Yes
IP SLAs - Scheduler	No	Yes	Yes
IP SLAs - Sub-millisecond Accuracy Improvements	No	Yes	Yes
IP SLAs - TCP Connect Operation	No	Yes	Yes
IP SLAs - UDP Based VoIP Operation	No	Yes	Yes
IP SLAs - UDP Echo Operation	No	Yes	Yes
IP SLAs - UDP Jitter Operation	No	Yes	Yes

**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
IP SLAs - Video Operations	No	Yes	Yes
IP SLAs - VoIP Threshold Traps	No	Yes	Yes
IP Summary Address for RIPv2	No	Yes	Yes
IP Unnumbered for VLAN-SVI interfaces	No	Yes	Yes
IPSG (IP Source Guard) v4	Yes	Yes	Yes
IPSG (IP Source Guard) v4 for Static Hosts	Yes	Yes	Yes
IPv4 Policy-Based Routing	No	Yes	Yes
IPv4 Policy-Based Routing with recursive next hop	No	Yes	Yes
IPv4 Routing: Static Hosts/Default Gateway	Yes	Yes	Yes
IPv6 ACL Wild Card Masking	Yes	Yes	Yes
IPv6 / v4 BFD with OSPF/ BGP/ EIGRP and Static	No	Yes	Yes
IPv6 BGP	No	No	Yes
IPv6 Bootstrap Router (BSR) Scoped Zone Support	No	No	Yes
IPv6 CNS Agents	Yes	Yes	Yes
IPv6 Config Logger	Yes	Yes	Yes
IPv6 First Hop Security (FHS): DHCPv6 Guard IPv6 Destination Guard IPv6 Snooping (Data Gleaning, per-limit Address Limit) IPv6 Neighbor Discovery (ND) Inspection IPv6 Neighbor Discovery Multicast Suppression IPv6 Router Advertisement (RA) Guard	Yes	Yes	Yes
IPv6 First Hop Security (FHS) Phase 2: Binding table recovery Lightweight DHCPv6 Relay Agent (LDRA) Neighbor Discovery (ND) Multicast Suppress Source and Prefix Guard <sup>3</sup> FHS EtherChannel Support	Yes	Yes	Yes

**Table 5** LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E

Feature	LAN Base	IP Base	Enterprise Services
IPv6 HSRP	No	Yes	Yes
IPv6 HTTP(S)	Yes	Yes	Yes
IPv6 ICMPv6	Yes	Yes	Yes
IPv6 ICMPv6 Redirect	Yes	Yes	Yes
IPv6 Interface Statistics	Yes	Yes	Yes
IPv6 IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	No	Yes	Yes
IPv6 Static Route support for Object Tracking	Yes	Yes	Yes
IPv6 TCL	Yes	Yes	Yes
IPv6 (Internet Protocol Version 6)	Yes	Yes	Yes
IPv6 Interface Statistics	Yes	Yes	Yes
IPv6 Access Services: DHCPv6 Relay Agent	No	Yes	Yes
IPv6: Anycast Address	Yes	Yes	Yes
IPv6 MLD Snooping v1 and v2	Yes	Yes	Yes
IPv6 MTU Path Discovery	Yes	Yes	Yes
IPv6 Multicast	No	Yes	Yes
IPv6 Multicast: Bootstrap Router (BSR)	No	Yes	Yes
IPv6 Multicast: Explicit Tracking of Receivers	No	Yes	Yes
IPv6 Multicast: MLD Access Group	No	Yes	Yes
IPv6 Multicast: Multicast Listener Discovery (MLD) Protocol, Versions 1 and 2	No	Yes	Yes
IPv6 Multicast: PIM Accept Register	No	Yes	Yes
IPv6 Multicast: PIM Embedded RP Support	No	Yes	Yes
IPv6 Multicast: PIM Source-Specific Multicast (PIM-SSM)	No	Yes	Yes
IPv6 Multicast: PIM Sparse Mode (PIM-SM)	No	Yes	Yes
IPv6 Multicast: Routable Address Hello Option	No	Yes	Yes

**Table 5** *LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E*

Feature	LAN Base	IP Base	Enterprise Services
IPv6 Multicast: RPF Flooding of Bootstrap Router (BSR) Packets	No	Yes	Yes
IPv6 Multicast: Scope Boundaries	No	Yes	Yes
IPv6 Neighbor Discovery Duplicate Address Detection	Yes	Yes	Yes
IPv6 OSPFv3 NSF/SSO	No	Yes <sup>4</sup>	Yes
IPv6 OSPFv3 Fast Convergence	No	Yes <sup>4</sup>	Yes
IPv6 PACL	Yes	Yes	Yes
IPv6 Policy-Based Routing	No	No	Yes
IPv6 RA Guard (Host Mode)	Yes	Yes	Yes
IPv6 Routing - EIGRP Support	No	No	Yes
IPv6 Routing: OSPF for IPv6 (OSPFv3)	No	Yes <sup>4</sup>	Yes
IPv6 Routing: RIP for IPv6 (RIPng)	No	Yes	Yes
IPv6 Routing: Route Redistribution	No	Yes	Yes
IPv6 Routing: Static Routing	Yes	Yes	Yes
IPv6 Security: Secure Shell SSH support over IPv6	Yes	Yes	Yes
IPv6 Services: AAAA DNS Lookups over an IPv4 Transport	No	Yes	Yes
IPv6 Services: Cisco Discovery Protocol (CDP) - IPv6 Address Family Support for Neighbor Information	Yes	Yes	Yes
IPv6 Services: DNS Lookups over an IPv6 Transport	Yes	Yes	Yes
IPv6 Services: Extended Access Control Lists	Yes	Yes	Yes
IPv6 Services: Standard Access Control Lists	Yes	Yes	Yes
IPv6 Stateless Auto-configuration	Yes	Yes	Yes
IPv6 Static Routing: Support for Tracking Objects	Yes	Yes	Yes
IPv6 Support for SGT/SGACL	Yes	Yes	Yes
IPv6 Switching: CEF Support	No	Yes	Yes
IPv6 Switching: CEFv6 Switched Automatic IPv4-compatible Tunnels (in software)	No	Yes	Yes

**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
IPv6 Switching: CEFv6 Switched ISATAP Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: Automatic 6to4 Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: Automatic IPv4-compatible Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: ISATAP Tunnel Support (in software)	No	Yes	Yes
IPv6 Tunneling: Manually Configured IPv6 over IPv4 Tunnels (in software)	No	Yes	Yes
IPv6 Virtual LAN Access Control List (VACL)	Yes	Yes	Yes
IPsecv3/IKEv2 (for management traffic only)	Yes	Yes	Yes
IS-IS for IPv4 and IPv6	No	No	Yes
ISSU (IOS In-Service Software Upgrade)	No	Yes	Yes
Jumbo Frames	Yes	Yes	Yes
Link Aggregation Control Protocol	Yes	Yes	Yes
LACP Min-Links	Yes	Yes	Yes
LACP Rate Fast	Yes	Yes	Yes
Layer 2 Control Packet	Yes	Yes	Yes
Layer 2 Protocol Tunneling (L2PT)	No	Yes	Yes
L2TP for LACP and PAgP	No	Yes	Yes
L2TP for UDLD	No	Yes	Yes
Layer 2 Traceroute	No	Yes	Yes
Layer 3 Multicast Routing (PIM SM, SSM, Bidir)	No	Yes	Yes
Link State Group	No	Yes	Yes
Link State Tracking	Yes	Yes	Yes
Loadsharing IP packets over more than six parallel paths	Yes	Yes	Yes
Local Proxy ARP	Yes	Yes	Yes

**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
Location MIBs	Yes	Yes	Yes
MAB with Configurable User Name/Password	Yes	Yes	Yes
MAB for Voice VLAN	Yes	Yes	Yes
MAC Address Notification	Yes	Yes	Yes
MAC Authentication Bypass	Yes	Yes	Yes
MAC Move and Replace	Yes	Yes	Yes
Medianet: AutoQoS SRND4 Macro	No	Yes	Yes
Medianet: Integrated Video Traffic Simulator (hardware-assisted IP SLA); IPSLA generator and responder	No	Yes	Yes
Medianet: Flow Metadata	No	Yes	Yes
Medianet: Media Service Proxy	No	Yes	Yes
Medianet: Media Monitoring (Performance Monitoring and Mediatrace)	No	Yes	Yes
Memory Threshold Notifications	Yes	Yes	Yes
Microflow policers	No	Yes	Yes
Modular QoS CLI (MQC)	Yes	Yes	Yes
Multi-authentication and VLAN Assignment	Yes	Yes	Yes
Multi-VRF Support (VRF lite)	No	No	Yes
Multicast BGP (MBGP)	No	No	Yes
Multicast Fast Switching Performance Improvement	No	Yes	Yes
Multicast HA (NSF/SSO) for IPv4&IPv6	No	Yes	Yes
Multicast Routing Monitor (MRM)	No	No	Yes
Multicast Source Discovery Protocol (MSDP)	No	Yes	Yes
Multicast Subsecond Convergence	No	Yes	Yes
Multicast VLAN Registration (MVR)	Yes	Yes	Yes
NAC - L2 IEEE 802.1x	Yes	Yes	Yes

**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
NAC - L2 IP	Yes	Yes	Yes
Named VLAN	Yes	Yes	Yes
ND Cache Limit/Interface	No	Yes	Yes
NEAT Enhancement: Re-Enabling BPDU Guard Based on User Configuration	Yes	Yes	Yes
NETCONF over SSHv2	Yes	Yes	Yes
Network Edge Access Topology (NEAT)	Yes	Yes	Yes
Network Time Protocol (NTP)	Yes	Yes	Yes
Network Time Protocol (NTP) master	Yes	Yes	Yes
Next Hop Resolution Protocol (NHRP)	No	No	Yes
NMSP Enhancements <ul style="list-style-type: none"> <li>• GPS support for location</li> <li>• Location at switch level</li> <li>• Local timezone change</li> <li>• Name value pair</li> <li>• Priority settings for MIBs</li> </ul>	No	Yes	Yes
No Service Password Recovery	Yes	Yes	Yes
No. of VLAN Support	2048	4096	4096
NSF - BGP	No	No	Yes
NSF - EIGRP	No	Yes	Yes
NSF - OSPF (version 2 only)	No	Yes	Yes
NSF/SSO (Nonstop Forwarding with Stateful Switchover)	No	Yes	Yes
NTP for IPv6	Yes	Yes	Yes
NTP for VRF aware	No	No	Yes
Object Group ACLs (OGACLs)	Yes	Yes	Yes
Object Tracking: IPv6 Route Tracking	No	Yes	Yes
Onboard Failure Logging (OBFL)	Yes	Yes	Yes



**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
Open Plug-N-Play Agent	Yes	Yes	Yes
OSPF	No	Yes <sup>4</sup>	Yes
OSPF v3 Authentication	No	Yes <sup>4</sup>	Yes
OSPF Flooding Reduction	No	Yes <sup>4</sup>	Yes
OSPF for Routed Access <sup>5</sup>	No	Yes	Yes
OSPF Incremental Shortest Path First (i-SPF) Support	No	Yes <sup>4</sup>	Yes
OSPF Link State Database Overload Protection	No	Yes <sup>4</sup>	Yes
OSPF Not-So-Stubby Areas (NSSA)	No	Yes <sup>4</sup>	Yes
OSPF Packet Pacing	No	Yes <sup>4</sup>	Yes
OSPF Shortest Paths First Throttling	No	Yes <sup>4</sup>	Yes
OSPF Stub Router Advertisement	No	Yes <sup>4</sup>	Yes
OSPF Support for Fast Hellos	No	Yes <sup>4</sup>	Yes
OSPF Support for Link State Advertisement (LSA) Throttling	No	Yes <sup>4</sup>	Yes
OSPF Support for Multi-VRF on CE Routers	No	Yes <sup>4</sup>	Yes
OSPF Update Packet-Pacing Configurable Timers	No	Yes <sup>4</sup>	Yes
PBR Support for Multiple Tracking Options	Yes	Yes	Yes
PBR with Object Tracking	No	Yes	Yes
Per Intf IGMP State Limit	Yes	Yes	Yes
Per Intf MrouteState Limit	Yes	Yes	Yes
Per Port Per VLAN Policing	Yes	Yes	Yes
Per-User ACL Support for 802.1X/MAB/Webauth users	Yes	Yes	Yes
Per-VLAN Learning	Yes	Yes	Yes
Permanent Right-to-Use (PRTU) license	Yes	Yes	Yes
PIM Dense Mode State Refresh	No	Yes	Yes
PIM Multicast Scalability	No	Yes	Yes

**Table 5** LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E

Feature	LAN Base	IP Base	Enterprise Services
PIM Version 1	No	Yes	Yes
PIM Version 2	No	Yes	Yes
PnP Agent	Yes	Yes	Yes
PoEP via LLDP	Yes	Yes	Yes
Port Security	Yes (supports 1024 MACs)	Yes (supports 3072 MACs)	Yes (supports 3072 MACs)
Port Security on Etherchannel Trunk Port	Yes	Yes	Yes
Port Security MAC Address Filtering	Yes	Yes	Yes
Pragmatic General Multicast (PGM)	No	Yes	Yes
Priority Queueing (PQ)	Yes	Yes	Yes
Private VLAN Promiscuous Trunk Port	Yes	Yes	Yes
Private VLAN Trunk Ports	Yes	Yes	Yes
Private VLANs	Yes	Yes	Yes
Propagation of Location Info over CDP	Yes	Yes	Yes
PVLAN over EtherChannel	Yes	Yes	Yes
PVST + (Per VLAN Spanning Tree Plus)	Yes	Yes	Yes
Q-in-Q	No	Yes	Yes
QoS Packet Marking	Yes	Yes	Yes
QoS Priority Percentage CLI Support	Yes	Yes	Yes
RADIUS	Yes	Yes	Yes
RADIUS Attribute 44 (Accounting Session ID) in Access Requests	Yes	Yes	Yes
RADIUS Change of Authorization	Yes	Yes	Yes
Rapid PVST+ Dispute Mechanism	Yes	Yes	Yes
Rapid-Per-VLAN-Spanning Tree Plus (Rapid-PVST+)	Yes	Yes	Yes
Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)	Yes	Yes	Yes
Reduced MAC Address Usage	Yes	Yes	Yes

**Table 5** *LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E*

<b>Feature</b>	<b>LAN Base</b>	<b>IP Base</b>	<b>Enterprise Services</b>
Redundancy Facility Protocol	Yes	Yes	Yes
Remote SPAN (RSPAN)	Yes	Yes	Yes
REP (Resilient Ethernet Protocol)	Yes	Yes	Yes
REP - No Edge Neighbor Enhancement	Yes	Yes	Yes
RIP v1	No	Yes	Yes
RMON events and alarms	Yes	Yes	Yes
RPR Mode for Catalyst 4500-E In-Chassis Redundant Supervisors with VSS	No	Yes	Yes
Secure CDP	Yes	Yes	Yes
Secure Copy (SCP)	Yes	Yes	Yes
Secure Shell SSH Version 2 Client Support	Yes	Yes	Yes
Secure Shell SSH Version 2 Server Support	Yes	Yes	Yes
Security Group ACL at Interface Level	Yes	Yes	Yes
Single Rate 3-Color Marker for Traffic Policing	Yes	Yes	Yes
Smart Install Director—Configuration-only Deployment and Smooth Upgrade	Yes	Yes	Yes
Smart Port	Yes	Yes	Yes
SMI Catalyst 4K Client	Yes	Yes	Yes
SNMP (Simple Network Management Protocol)	Yes	Yes	Yes
SNMP Inform Request	Yes	Yes	Yes
SNMP Manager	Yes	Yes	Yes
SNMPv2C	Yes	Yes	Yes
SNMPv3 - 3DES and AES Encryption Support	Yes	Yes	Yes
SNMPv3 (SNMP Version 3)	Yes	Yes	Yes
Source Specific Multicast (SSM)	No	Yes	Yes
Source Specific Multicast (SSM) - IGMPv3,IGMP v3lite, and URD	No	Yes	Yes

**Table 5** LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E

Feature	LAN Base	IP Base	Enterprise Services
Source Specific Multicast (SSM) Mapping	No	Yes	Yes
SPAN (# of bidirectional sessions) – Port Mirroring	Yes (4 bidirectional sessions)	Yes (16 bidirectional sessions)	Yes (16 bidirectional sessions)
SPAN ACL Filtering for IPv6	Yes	Yes	Yes
Span Enhancement: Packet Type and Address Type Filtering	Yes	Yes	Yes
Spanning Tree Protocol (STP)	Yes	Yes	Yes
Spanning Tree Protocol (STP) Backbone Fast Convergence Bridge Assurance Dispute Mechanism Loop Guard Portfast PortFast BPDU Filtering Portfast BPDU Guard Portfast Support for Trunks PVST+ Simulation Root Guard STP Extension Uplink Fast Convergence Uplink Load Balancing	Yes	Yes	Yes
Stateful Switchover	Yes	Yes	Yes
Standard IP Access List Logging	Yes	Yes	Yes
Standby Supervisor Port Usage	Yes	Yes	Yes
Sticky Port Security	Yes	Yes	Yes
Sticky Port Security on Voice VLAN	Yes	Yes	Yes
Storm Control	Yes	Yes	Yes
Storm Control - Per-Port Multicast Suppression	Yes	Yes	Yes
STP Syslog Messages	Yes	Yes	Yes

**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
Stub IP Multicast Routing	No	Yes	Yes
Sub-second UDLD	Yes	Yes	Yes
SVI (Switch Virtual Interface) Autostate Exclude	Yes	Yes	Yes
Switch and IP Phone Security Interaction	Yes	Yes	Yes
Switch Port Analyzer (SPAN)	Yes	Yes	Yes
Switch Port Analyzer (SPAN) - CPU Source	Yes	Yes	Yes
Syslog over IPV6	Yes	Yes	Yes
System Logging - EAL4 Certification Enhancements	No	Yes	Yes
TACACS SENDAUTH function	Yes	Yes	Yes
TACACS Single Connection	Yes	Yes	Yes
TACACS+	Yes	Yes	Yes
TACACS+ and Radius for IPv6-	Yes	Yes	Yes
TCAM4 - Dynamic Multi-Protocol	Yes	Yes	Yes
TCAM4 - Service-Aware Resource Allocation	Yes	Yes	Yes
Time Domain Reflectometry (TDR) <sup>6</sup>	Yes	Yes	Yes
Time-Based Access Lists	Yes	Yes	Yes
Time-Based Access Lists Using Time Ranges (ACL)	Yes	Yes	Yes
Trusted boundary (extended trust for CDP devices)	Yes	Yes	Yes
UDI - Unique Device Identifier	Yes	Yes	Yes
Uni-Directional Link Routing (UDLR)	No	Yes	Yes
Unicast Mac Filtering	Yes	Yes	Yes
Unicast Reverse Path Forwarding (uRPF)	No	Yes	Yes
Unidirectional Ethernet	Yes	Yes	Yes
UniDirectional Link Detection (UDLD)	Yes	Yes	Yes
UDP Forwarding Support for IP Redundancy Virtual Router Group	Yes	Yes	Yes

**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
Virtual Router Redundancy Protocol (VRRP) for IPv4	No	Yes	Yes
Virtual Switching System (VSS)	No	Yes (SUP7E and SUP8E only)	Yes (SUP7E, SUP7LE, SUP8E, and SUP8LE)
Virtual Switching System (VSS): Layer 2 Protocol Tunneling, VLAN Translation, and Q-in-Q	No	Yes	Yes
Virtual Switching System (VSS): REP, Flexlinks, UDLD, and Fast UDLD	No	Yes	Yes
Virtual Trunking Protocol (VTP) - Pruning	Yes	Yes	Yes
VLAN Access Control List (VACL)	Yes	Yes	Yes
VLAN MAC Address Filtering	Yes	Yes	Yes
VLAN Mapping (VLAN Translation)	No	Yes	Yes
VLAN Switching and Selective QinQ on the Same Port	No	Yes	Yes
VRF-aware Copy Commands	No	Yes	Yes
VRF-aware PBR	No	No	Yes
VRF-aware TACACS+	No	No	Yes
VRF-aware WCCP for IPv4 traffic	No	No	Yes
VRF-aware WCCP for IPv6 traffic	No	No	Yes
VRF-lite for IPv6 on OSPF/ BGP/ EIGRP	No	No	Yes
VRRPv3: Object Tracking Integration	No	Yes	Yes
VRRPv3 Protocol Support	No	Yes	Yes
VTP (Virtual Trunking Protocol) Version 2	Yes	Yes	Yes
VTP Version 3	Yes	Yes	Yes
WCCP Version 2	No	Yes	Yes
WCCP Version 2 on VSS	No	Yes	Yes
WCCP Version 2 for IPv6	No	Yes	Yes
Web Authentication Proxy	Yes	Yes	Yes

**Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and Supervisor Engine 8L-E**

Feature	LAN Base	IP Base	Enterprise Services
Web Authentication Redirection to Original URL	Yes	Yes	Yes
Webauth Enhancements	Yes	Yes	Yes
Wireless Termination with VSS (Supervisor Engine 8-E)	No	Yes	Yes
Wired Guest Access <sup>7</sup>	No	Yes	Yes
Wireshark-based Ethernet Analyzer	No	Yes	Yes
XML-PI	Yes	Yes	Yes

- Supervisor Engine 7-E, and Supervisor Engine 8-E, Supervisor Engine 8L-E; IP Base. Supervisor Engine 7L-Ent Services
- EEE 802.1t—An IEEE amendment to IEEE 802.1D that includes extended system ID, long path cost, and PortFast.
- When either Source or Prefix Guard for IPv6 is enabled, ICMPv6 packets are unrestricted on all Catalyst 4500 series switch platforms running IOS Cisco Release 15.2(1)E. All other traffic types are restricted.
- IP Base supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 200 dynamically learned routes.
- OSPF for Routed Access supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 1000 dynamically learned routes.
- TDR is not supported on 46xx linecards.
- Wired Guest Access is supported only in wireless mode on Supervisor Engine 8-E, when the switch functions as a mobility agent and or a mobility controller.

## OpenFlow Version and Cisco IOS Release Support

The following table provides OpenFlow compatibility information for the Cisco Catalyst 4500-E Series Switches. The OVA package is available for download in the same location as your system image (.bin) file, on cisco.com



### Note

The OVA package is compatible only with its corresponding system image file name - as listed in the table below. Do not use an older version of the OVA package with a newer system image file, or a newer OVA package with an older system image file.

**Table 6 Image Support for OpenFlow Version and Cisco IOS Release Support for Cisco OpenFlow Plug-In**

Platform	Cisco IOS Release	Cisco OpenFlow Plug-In Version	Cisco OpenFlow Plug-In	Image Name
Catalyst 4500-E Series Switches with Supervisor Engine 8-E/ 8L-E	IOS XE 3.8.1E	2.0.2	ofa-2.0.2-r2-cat4500es8-SPA-k9.ova	cat4500es8-universalk9.SPA.03.08.01.E.152-4.E.bin

Platform	Cisco IOS Release	Cisco OpenFlow Plug-In Version	Cisco OpenFlow Plug-In	Image Name
Catalyst 4500-E Series Switches with Supervisor Engine 8-E	IOS XE 3.8.0E	2.0.2	ofa-2.0.2-r2-cat4500es8-SPA-k9.ova	cat4500es8-universalk9.SPA.03.08.00.E.152-4.E.bin
Catalyst 4500-E Series Switches with Supervisor Engine 7-E/ 7L-E	IOS XE 3.8.0E	2.0.2	ofa-2.0.2-r2-cat4500-SPA-k9.ova	cat4500e-universalk9.SPA.03.08.00.E.152-4.E.bin

## MIB Support

For information on MIB support, please refer to this URL:

<ftp://ftp.cisco.com/pub/mibs/supportlists/cat4000/cat4000-supportlist.html>

## Features Not Supported on the Cisco Catalyst 4500-E Series Switch

The following features are not supported on a Catalyst 4500-E series switch with Supervisor Engine 7-E and Supervisor Engine 7L-E:

- CISCO-IETF-IP-FORWARD-MIB
- CISCO-IETF-IP-MIB
- LLDP HA
- WCCP Version 1
- SSH Version 1

## Orderable Product Numbers

**Table 7** Cisco IOS XE Software Release 3.8.0E Product Numbers and Images for the Catalyst 4500E Series Switch

Product Number	Description	Image
S45EULPE-S8-38E	CAT4500e SUP8e Universal NoMACSEC Image	cat4500es8-universalk9npe
S45EUK9-S8-38E	CAT4500e SUP8e Universal Crypto Image	cat4500es8-universalk9
S45EUK9-S7-38E	CAT4500e SUP7-E/SUP7L-E Universal Crypto Image	cat4500e-universalk9
S45EUN-S7-38E	CAT4500e SUP7-E/SUP7L-E Universal No MACSEC Image	cat4500e-universalk9npe
S45EU-S8-38E	CAT4500e SUP8e Universal Image	cat4500es8-universal



**Table 7** Cisco IOS XE Software Release 3.8.0E Product Numbers and Images for the Catalyst 4500E Series Switch

Product Number	Description	Image
S45EU-S7-38E	CAT4500e SUP7-E/SUP7L-E Universal Image	cat4500e-universal

## New and Changed Information

The Cisco IOS XE Release 3.8.xE Documentation Roadmap provides quick and easy access to all relevant documentation for specific platforms. Look for Quick Links to Platform Documentation on the respective platform documentation pages. For more information, see <http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-3e/tsd-products-support-series-home.html>.

These sections describe the new and changed information for the Catalyst 4500E Series Switch running Cisco IOS XE software:

- “New Features in Cisco IOS XE Release 3.8.9E” section on page 33
- “New Features in Cisco IOS XE Release 3.8.8E” section on page 33
- “New Features in Cisco IOS XE Release 3.8.7E” section on page 33
- “New Features in Cisco IOS XE Release 3.8.6E” section on page 33
- “New Features in Cisco IOS XE Release 3.8.5aE” section on page 34
- “New Features in Cisco IOS XE Release 3.8.5E” section on page 34
- “New Features in Cisco IOS XE Release 3.8.3E” section on page 34
- “New Features in Cisco IOS XE Release 3.8.2E” section on page 35
- “New Features in Cisco IOS XE Release 3.8.1E” section on page 36
- “New Features in Cisco IOS XE Release 3.8.0E” section on page 38

### New Features in Cisco IOS XE Release 3.8.9E

There are no new features in this release.

### New Features in Cisco IOS XE Release 3.8.8E

- There are no new features in this release.

### New Features in Cisco IOS XE Release 3.8.7E

- There are no new features in this release.

### New Features in Cisco IOS XE Release 3.8.6E

- There are no new features in this release.

## New Features in Cisco IOS XE Release 3.8.5aE

There are no new features in this release.

## New Features in Cisco IOS XE Release 3.8.5E

There are no new features in this release.

## New Features in Cisco IOS XE Release 3.8.4E

There are no new features in this release.

## New Features in Cisco IOS XE Release 3.8.3E

### New Software Features


**Table 8** *New Software Features in this Release*

Feature Name	Description
Support for mDNS with Application Policy Infrastructure Controller Enterprise Module (APIC-EM) platform on Cisco Catalyst 4500 E-Series Supervisor Engine 8E	mDNS provides service announcement and query for specific services. The SD-Bonjour application is designed on Cisco APIC-EM platform to enable service discovery across an enterprise network while relieving load from the IOS devices. Services learnt on access layer are unicasted to APIC-EM and stored. This stored data is sent to other clients on a different subnet across the network as per the request.

## New Features in Cisco IOS XE Release 3.8.2E

### New Software Features

**Table 9** *New Software Features in this Release*

Feature Name	Description
Support for -B Domain	<p>The FCC (USA) rule-making on 5-GHz released on April 1, 2014, (FCC 14-30 Report and Order) goes into effect for products that are sold or shipped on or after June 2, 2016. Cisco APs and Cisco WLCs will comply with the new rules by supporting the new regulatory domain (-B) for the US and will create new AP SKUs that are certified under the new rules. Examples of new rules include new 5-GHz band channels permitted for outdoor use, and transmission (Tx) power level increased to 1W for indoor, outdoor, and point-to-point transmissions.</p> <div style="text-align: center;">  </div> <p><b>Note</b> Cisco APs and Cisco WLCs that are in the -A domain category can continue to operate and even coexist with -B domain devices without any issues.</p> <hr/> <p>We recommend that you upgrade Cisco APs and Cisco WLCs to the appropriate software release that supports -B domain.</p>
Support is added for these access points:	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Aironet 1850 Series Access Points</a></li> <li>• <a href="#">Cisco Aironet 1830 Series Access Points</a></li> </ul>

# New Features in Cisco IOS XE Release 3.8.1E

## New Hardware Features

**Table 10** *New Hardware Features in this Release*

Feature Name	Description
WS-X45-Sup8L-E	<p>Support for Cisco Catalyst 4500 E-Series Supervisor Engine 8L-E.</p> <p>The supervisor engine is supported on the Catalyst 4503-E, Catalyst 4506-E, Catalyst 4507R+E, Catalyst 4507R-E<sup>1</sup> switch chassis.</p> <p>For more information, see the following documents on cisco.com:</p> <ul style="list-style-type: none"> <li>• <a href="#">Installation and Configuration Note for the Cisco Catalyst 4500 E-Series Supervisor Engine 8L-E.</a></li> <li>• <a href="#">Catalyst 4500 E-Series Installation Guide</a></li> </ul>
Support for BX SFP and SFP+ Transceivers	<p>The following new BX SFP and SFP+ transceivers are supported on the Catalyst 4500-E switches with Supervisor Engine 8L-E, WS-X4712-SFP+E, WS-X4606-X2-E (Using a Cisco OneX Converter Module), and WS-X4602-10GE (Using a Cisco OneX Converter Module).</p> <ul style="list-style-type: none"> <li>• SFP-10G-BXD-I</li> <li>• SFP-10G-BXU-I</li> <li>• SFP-10G-BX40D-I</li> <li>• SFP-10G-BX40U-I</li> </ul> <p>The following new transceivers are supported on the on the Catalyst 4500-E switches with Supervisor Engine 8L-E, and with modules WS-X4712-SFP+E, WS-X4748-SFP-E, WS-X4624-SFP-E, WS-X4602-10GE (Using a Cisco TwinGig Converter Module), WS-X4724-SFP-E, WS-X4712-SFP-E, WS-X4612-SFP-E, WS-X4640-CSFP-E, WS-X4606-X2-E (Using a Cisco TwinGig Converter Module), WS-X4448-GB-SFP, WS-X4724-SFP-E, WS-X4712-SFP-E, and WS-X4612-SFP-E.</p> <ul style="list-style-type: none"> <li>• GLC-BX40-D-I</li> <li>• GLC-BX80-D-I</li> <li>• GLC-BX40-U-I</li> <li>• GLC-BX80-U-I</li> <li>• GLC-BX40-DA-I</li> </ul>

1. To support Supervisor Engine 8L-E, the Cisco Catalyst 4507R-E Switch chassis must have hardware revision 2.0 or higher.

## New Software Features

**Table 11**      *New Software Features in this Release*

Feature Name	Description
ERSPAN	<p>The Cisco Encapsulated Remote Switched Port Analyzer (ERSPAN) feature allows you to monitor traffic on source ports or source VLANs, on remote destination switches or probes across the network. ERSPAN uses a generic routing encapsulation tunnel (GRE) tunnel to carry traffic between switches.</p> <p>The feature is supported on supervisor engines—7E, 7LE, 8E, and 8LE. (LAN Base, IP Base, and Enterprise Services)</p>
Limiting Login	<p>The Limiting Login feature helps network administrators to limit the login attempt of users to a network. When a user fails to successfully login to a network within a configurable number of attempts within a configurable time limit, the user can be blocked. This feature is enabled only for local users and not for remote users. You need to configure the <b>aaa authentication rejected</b> command in global configuration mode to enable this feature.</p>
x.509v3 with SSH Authentication	<p>This feature uses the public key algorithm (PKI) for server and user authentication, and allows the Secure Shell (SSH) protocol to verify the identity of the owner of a key pair via digital certificates, signed and issued by a Certificate Authority (CA).</p>

# New Features in Cisco IOS XE Release 3.8.0E

## New Hardware Features

**Table 12** *New Hardware Features in this Release*

Feature Name	Description
Support for BX SFP and SFP+ Transceivers	<p>The following new BX SFP and SFP+ transceivers are supported on the Catalyst 4500-E switches with Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, WS-X4712-SFP+E, WS-X4606-X2-E (Using a Cisco OneX Converter Module), and WS-X4602-10GE (Using a Cisco OneX Converter Module).</p> <ul style="list-style-type: none"> <li>• SFP-10G-BXD-I</li> <li>• SFP-10G-BXU-I</li> <li>• SFP-10G-BX40D-I</li> <li>• SFP-10G-BX40U-I</li> </ul> <p>The following new transceivers are supported on the on the Catalyst 4500-E switches with Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E, and with modules WS-X4712-SFP+E, WS-X4748-SFP-E, WS-X4624-SFP-E, WS-X4602-10GE (Using a Cisco TwinGig Converter Module), WS-X4724-SFP-E, WS-X4712-SFP-E, WS-X4612-SFP-E, WS-X4640-CSFP-E, WS-X4606-X2-E (Using a Cisco TwinGig Converter Module), WS-X4448-GB-SFP, WS-X4724-SFP-E, WS-X4712-SFP-E, and WS-X4612-SFP-E.</p> <ul style="list-style-type: none"> <li>• GLC-BX40-D-I</li> <li>• GLC-BX80-D-I</li> <li>• GLC-BX40-U-I</li> <li>• GLC-BX80-U-I</li> <li>• GLC-BX40-DA-I</li> </ul>

## New Software Features (Wired)

**Table 13** *New Software Features (Wired) in this Release*

Feature Name	Description
Auto Identity	<p>Provides a set of built-in policies at the global configuration and interface configuration modes. The Auto Identity feature uses the Cisco Common Classification Policy Language (C3PL)-based configuration that significantly reduces the number of commands used to configure both authentication methods and interface-level commands. The Auto Identity feature provides a set of built-in policies that are based on policy maps, class maps, parameter maps, and interface templates.</p> <p>(IP Base and Enterprise Services)</p>
Bidirectional Forwarding Detection (BFD) for Intermediate System to Intermediate System (IS-IS)	<p>BFD Support for the IS-IS protocol, on IPv4 and IPv6.</p> <p>(Enterprise Services)</p>

**Table 13**      **New Software Features (Wired) in this Release**

Feature Name	Description
Cisco TrustSec—SGACL Logging and Statistics	Option to enable logging of Security Group-Based Access Control (SGACL) information and Access Control Entry (ACE) statistics. The logged information includes the source and destination security group tag, the SGACL policy name, packet protocol type, the action performed on the packet, and ACE matches. For more information, see the <a href="#">Cisco TrustSec Switch Configuration Guide</a> on cisco.com. (IP Base and Enterprise Services)
LACP Min-Links	Allows you to specify the minimum number of active ports that must be in the link-up state and bundled in an EtherChannel for the port channel interface to transition to the link-up state. (LAN Base, IP Base, and Enterprise Services)
Link State Group	The upper limit of the link state group number value is now increased (from 10) to 20. You can configure upto 20 link state groups per switch. (IP Base, and Enterprise Services)
Named VLAN	Option to specify a VLAN name for access and voice VLAN. (LAN Base, IP Base, and Enterprise Services)
Policy-Based Routing (PBR) with Object Tracking	Support for a new command <b>set ip next-hop verify-availability</b> , to use PBR with object tracking, to verify the reachability of the next-hop IP address to which to forward packets, using an Internet Control Message Protocol (ICMP) ping as the verification method. This feature is supported only on IPv4 PBR and is not supported on IPv6 PBR, and PBR on VSS and VRF. (IP Base and Enterprise Services)
Private VLAN (PVLAN) Support on LAN Base	PVLAN is now supported on LAN Base images. (LAN Base)
Rapid PVST+ as Default	Rapid PVST+ is now the default spanning-tree mode used on all Ethernet port-based VLANs. (LAN Base, IP Base, and Enterprise Services)
Resilient Ethernet Protocol (REP) Enhancements	Option to configure an administrative VLAN for each segment. This allows you to configure any number of administrative VLANs as long as it is per segment. (LAN Base, IP Base, Enterprise Services)
RPR Mode for Catalyst 4500-E In-Chassis Redundant Supervisors with VSS	With Quad-Supervisor VSS, each chassis in the VSS can now support an in-chassis standby supervisor (ICS) that operates in RPR mode. (IP Base and Enterprise Services)

**Table 13**      **New Software Features (Wired) in this Release**

Feature Name	Description
Spanning Tree Protocol (STP) Enhancements	<p>Bridge Assurance—Protects the network from bridging loops that are caused by that are caused by unidirectional links, or a malfunctioning switch. Bridge Assurance is enabled by default, and applies only to PortFast network ports.</p> <p>Detecting UniDirectional Link Failures (or the STP Dispute Mechanism)—The switch port detects unidirectional link failures by checking the consistency of the port role and state of the BPDUs received. When a conflict is detected, the designated port reverts to a blocking state. This feature does not require any user configuration.</p> <p>PVST+ Simulation—This is now user-configurable. You can enable or disable this per port, or globally. PVST+ simulation is enabled by default. It allows seamless interoperability between MST and Rapid PVST+.</p> <p>(LAN Base, IP Base, Enterprise Services)</p>
Stateful Switchover (SSO)	<p>SSO is now supported on LAN Base Images.</p> <p>(LAN Base)</p>
Storm Control Enhancements	<p>Option to specify the threshold level for broadcast traffic in bits per second (bps) and packets per second (pps).</p> <p>(LAN Base, IP Base, and Enterprise Services)</p>
UDP Forwarding Support for IP Redundancy Virtual Router Group	<p>UDP broadcast is now limited to the active router in the Virtual Router Group (VRG). Only a VRG that is implemented with the Hot Standby Routing Protocol (HSRP) is supported</p> <p>(IP Base and Enterprise Services)</p>
VLAN Switching and Selective QinQ on the Same Port	<p>Option to disable default behavior of dropping non-translated VLANs. When configuring VLAN mapping for selective Q-in-Q on a trunk port, you now have the option to specify that packets that do not match, should not be dropped (Enter the <b>no switchport vlan mapping default drop</b> command).</p> <p>(IP Base, and Enterprise Services)</p>
VRF-aware WCCP for IPv4 traffic	<p>WCCP now supports IPv4 traffic redirection to and from Virtual Routing and Forwarding (VRF) interfaces.</p> <p>(Enterprise Services)</p>
VRF-aware WCCP for IPv6 traffic	<p>WCCP now supports IPv6 traffic redirection to and from Virtual Routing and Forwarding (VRF) interfaces.</p> <p>(Enterprise Services)</p>
VSS	<p>The REP, Flexlinks, Unidirectional Link Detection (UDLD), and Fast UDLD features are now supported on VSS.</p> <p>(IP Base and Enterprise Services)</p>
WCCP Version 2 for IPv6	<p>WCCPv2 now supports IPv6 traffic.</p> <p>(IP Base and Enterprise Services)</p>



## New Software Features (Wireless)

**Table 14** *New Software Features (Wireless) in this Release*

Feature Name	Description
Wireless Termination with VSS	Cisco Catalyst 4500 E-Series Supervisor Engine 8-E (WS-X45-Sup8-E) now supports wireless features in VSS. It can be operated as a mobility agent (MA) or mobility controller (MC). An MA maintains CAPWAP tunnels of directly connected access points and client mobility state machine. An MC provides mobility management services for group roaming events.  (IP Base and Enterprise Services)

## Cisco IOS XE to Cisco IOS

As [Table 15](#) shows, each version of Cisco IOS XE has an associated Cisco IOS version:

**Table 15** *Cisco IOS XE to Cisco IOS*

Cisco IOS XE Version	Cisco IOS Version	Cisco Wireless Control Module Version	Access Point Version
03.1.0SG	15.0(1)XO	-	-
03.1.1SG	15.0(1)XO1	-	-
03.2.0SG	15.0(2)SG	-	-
03.3.0SG	15.1(1)SG	-	-
03.3.1SG	15.1(1)SG1	-	-
03.4.0SG	15.1(2)SG	-	-
03.5.0E	15.2(1)E	-	-
03.6.0E	15.2(2)E	-	-
03.7.0E	15.2(3)E	10.3.100.0	15.3(3)JNB
03.8.0E	15.2(4)E	10.3.100.0	15.3(3)JNB
03.8.1E	15.2(4)E1	10.4.111.0	15.3(3)JNC1

## Wireless Related Information

- [Wireless Web UI Software Requirements](#)
- [Access Points and Mobility Services Engine](#)
- [Compatibility Matrix](#)
- [Interoperability with Other Client Devices](#)
- [Important Notes](#)

## Wireless Web UI Software Requirements

- Operating Systems
  - Windows 7
  - Windows 8
  - Mac OS X 10.8
- Browsers
  - Google Chrome—Version 35
  - Microsoft Internet Explorer—Versions 10 or 11
  - Mozilla Firefox—Version 30
  - Safari—Version 6.1

## Access Points and Mobility Services Engine

Table 16 lists the supported products for the wireless features.

**Table 16** Supported Wireless Products

Product	Platform Supported
Access Point	Cisco Aironet 700, 700W, 1040, 1140, 1260, 1530, 1570, 1600, 1700, 2600, 2700, 3500, 3600, 3700
Mobility Services Engine	3355, Virtual Appliance

Table 17 lists the specific supported Cisco access point models.

**Table 17** Supported Access Points

Access Points	
Cisco Aironet 700 Series	AIR-CAP702W-x-K9
	AIR-CAP702I-x-K9
	AIR-CAP702I-xK910
Cisco Aironet 700W Series	AIR-CAP702Wx-K9
	AIR-CAP702W-xK910
Cisco Aironet 1040 Series	AIR-AP1041N
	AIR-AP1042N
	AIR-LAP1041N
	AIR-LAP1042N
Cisco Aironet 1140 Series	AIR-AP1141N
	AIR-AP1142N
	AIR-LAP1141N
	AIR-LAP1142N

**Table 17** *Supported Access Points (continued)*

<b>Access Points</b>	
Cisco Aironet 1260 Series	AIR-LAP1261N
	AIR-LAP1262N
	AIR-AP1261N
	AIR-AP1262N
Cisco Aironet 1530 Series	AIR-CAP1532I-x-K9
	AIR-CAP1532E-x-K9
Cisco Aironet 1570 Series	AIR-AP1572EAC-A-K9
	AIR-AP1572ECx-A-K9
	AIR-AP1572ICx-A-K9
Cisco Aironet 1600 Series	AIR-CAP1602E
	AIR-CAP1602I
Cisco Aironet 1700 Series	AIR-CAP1702I-x-K9
	AIR-CAP1702I-xK910
Cisco Aironet 2600 Series	AIR-CAP2602E
	AIR-CAP2602I
Cisco Aironet 2700 Series	AIR-CAP2702I-x-K9
	AIR-CAP2702E-x-K9
Cisco Aironet 3500 Series	AIR-CAP3501E
	AIR-CAP3501I
	AIR-CAP3501P
	AIR-CAP3502E
	AIR-CAP3502I
	AIR-CAP3502P
Cisco Aironet 3600 Series	AIR-CAP3602E
	AIR-CAP3602I
Cisco Aironet 3700 Series	AIR-CAP3702I
	AIR-CAP3702E
	AIR-CAP3702P

## Compatibility Matrix

[Table 18](#) lists the software compatibility matrix.

**Table 18**      **Software Compatibility Matrix**

Cisco 5700 WLC	Catalyst 3850	Catalyst 3650	Catalyst 4500E with Sup 8-E	Cisco 5508 WLC or WiSM2	MSE	ISE	ACS	Cisco PI
03.07.00E	03.07.00E	03.07.00E	03.08.00E	8.0 7.6	8.0	1.4	5.2 5.3	3.0

For more information on the compatibility of wireless software components across releases, see the [Cisco Wireless Solutions Software Compatibility Matrix](#).

## Interoperability with Other Client Devices

This section describes the interoperability of this version of the switch software release with other client devices.

[Table 19](#) lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

**Table 19**      **Client Types**

Client Type and Name	Version
<b>Laptop</b>	
Intel 4965	11.5.1.15 or 12.4.4.5, v13.4
Intel 5100/6300	v14.3.0.6
Intel 6205	v15.10.5.1
Intel 6235	V15.10.5.1
Intel 6300	v15.10.4.2
Intel 7260(11AC)	17.0.0.34, Windows 8.1
Dell 1395/1397	XP/Vista: 5.60.18.8 Win7: 5.30.21.0
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1515 (Atheros)	8.0.0.239
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	v5.100.235.12
Cisco CB21	v1.3.0.532
Atheros HB95	7.7.0.358
MacBook Pro (Broadcom)	5.10.91.26
Broadcom 4360(11AC)	6.30.163.2005
Macbook Air (11AC)	10.9.3
Macbook Air	10.9.3
<b>Handheld Devices</b>	
Apple iPad	iOS 5.0.1
Apple iPad2	iOS 6.0.1

**Table 19**      *Client Types (continued)*

<b>Client Type and Name</b>	<b>Version</b>
Apple iPad3	8.0.2(12A405)
Apple iPad Air	8.0.2(12A405)
Apple iPad Mini	8.0.2(12A405)
Samsung Galaxy Tab	Android 3.2
Intermec CK70	Windows Mobile 6.5 / 2.01.06.0355
Intermec CN50	Windows Mobile 6.1 / 2.01.06.0333
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R
<b>Phones and Printers</b>	
Cisco 7921G	1.4.2.LOADS
Cisco 7925G	1.4.2.LOADS
Ascom i75	1.8.0
Spectralink 8030	119.081/131.030/132.030
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.345
Apple iPhone 4	iOS 6.0.1
Apple iPhone 4S	8.0.2(12A405)
Apple iPhone 5s	8.0.2(12A405)
Apple iPhone 5c	8.0.2(12A405)
Apple iPhone 6	8.0.2(12A405)
Ascom i62	2.5.7
HTC Sensation	Android 2.3.3
Samsung Galaxy S II	Android 2.3.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Samsung Galaxy Nexus	Android 4.0.2
Samsung Galaxy S4 (GT-I9500)	4.4.2
Samsung Galaxy Note (SM-900)	4.4.2

## Important Notes

- Starting with Cisco IOS XE Release 3.8.5, you must use switch ports as uplink ports on the Catalyst 4500E Series Switch for mobility tunnels to work.
- On a Catalyst 4500E Series Switch with Supervisor Engine 8-E, to boot the system in wireless mode, you have to set the configuration register to value 0x2102. For more information, see section [Modifying the Configuration Register Value for Wireless Mode](#), in the software configuration guide.
- Software expand running command is not available. We recommend that you use software expand file command instead.

- Redundancy mode rpr is not available in wireless enabled mode.
- Location keyword to fetch the data from active/active-dc/stby/stby-dc
- Wireless mode shows dc boot status and errors (if any) during boot up.

```
Status (Success):
Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.
(http://www.gnu.org/licenses/gpl-2.0.html) For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
```

```
# # ## ##### # # # # # ##
# # # # # # ## # # ## # # #
# # # # # # # # # # # # # #
# ## # ##### ##### # # # # # ##
## ## # # # # # ## # # ## # #
# # # # # # # # # # # # ##
```

```
Daughter Card is booting.. Please stand by.....
Daughter Card is ready, continuing in wireless mode..
```

- Default configurations and internal interfaces are created. Details on default policy-map:

```
*Dec 4 01:57:09.019: %LINK-3-UPDOWN: Interface Port-channel256, changed state to up
*Dec 4 01:57:11.359: %LINK-3-UPDOWN: Interface Port-channel255, changed state to up

Interfaces TengigabitEthernet <supervisor-slot#>/internal-port#
Internal port#: 9-16.
```

No configuration is allowed on internal interfaces.

Status/Stats of internal ports are visible under service internal command.

Boot Failure messages:

- DC communication failures:

```
Daughter Card is booting.. Please stand by.....
!!! DAUGHTER CARD BOOT FAILED (DC Boot base package timeout), REBOOTING..!!!
```

- DC Programming Failures:

```
Daughter Card is booting.. Please stand by.....
!!! DAUGHTER CARD BOOT FAILED (DC Bootloader upgrade failed), REBOOTING..!!!

!!! DAUGHTER CARD FPGA UPGRADE FAILED!(FPGA READ HANG),Rebooting.. !!!
!!! DAUGHTER CARD BOOT FAILED (BOOTLOADER UPGRADE SKIPPED), REBOOTING..!!!
```

- Unsupported License:

```
-----

WARNING!!

License level incompatible to bring up daughtercard
```

```
Daughter Card is disabled!
```

```
Activate ipbase or entservices license to enable daughtercard
```

- 
- Restrictions:
    - Supported only in ipbase and entservices license.
    - Supported only in install mode.
    - Supported only in cat4500es8-universalk9\* (Crypto) images
    - Requires rommon version 15.1(1r)SG5 or later
    - Not supported in VSS
    - SUP7E mode not supported
  - Daughter card logs/crashinfo
    - DC bootup logs are stored in bootflash (max 5 files, 1 per reload) with **dc\_console\_log-yyyymmdd-hhmmss-UTC** format.
    - After DC becomes operational, the logs are forwarded to BB's syslog. DC logs have a prefix of DC-SLOT<slot-no>:
    - DC crash info and system reports are stored at crashinfo-dc: and slavecrashinfo-dc: for active-dc and stby-dc respectively
  - DC can be disabled in install boot via “hw-module daughtercard disable” configuration. However, you must save the configuration and reload the system for this to take effect.
  - AP Joining the WLC:
    - A new AP, which has only factory default configurations, sends an L3 Broadcast Discovery message to learn and discover a WLC. Then the WLCs in the broadcast domain respond to this request. This request also has the number of APs they can support and how many APs are currently connected. The AP then would send a Join message to the least loaded WLC among the list.
    - When there is an explicit primary WLC IP address configured on the AP, the AP sends a unicast WLC discovery message to this specific WLC. There could also be WLCs that the AP learned about in its past associations with the WLCs and it would send a Unicast Discovery to these WLCs too. After the WLCs respond to this query, it matches with the primary WLC name and IP address and if the match is found, it will join the WLC. If there is an invalid WLC name or IP, then it will not match and it will join the other WLCs that would have responded to the unicast query. If no other WLC responded to the AP, it would send an L3 broadcast discovery message again.
    - There is a difference in behavior between how the Sup 8-E based MA or MC handles the Unicast L3 Discovery packet as compared to the Catalyst 3850 Switch in MA or MC mode.  
 On Catalyst 3850 Switches—Any packet received on the management VLAN is terminated and not forwarded to the unicast IP address in the discovery even if the address does not belong to itself. When a primary base IP of the WLC is configured, the MA does not forward the unicast packets and the AP therefore falls back to sending a broadcast discovery packet which terminates on the Catalyst 3850 Switch.

On Sup 8-E—On the Sup 8-E MA, however, the unicast discovery packet, if received on the management VLAN, is forwarded to the right destination based on the IP address in the discovery packet. Therefore, it reaches the destined WLC and joins it and not the SUP 8-E if the destination IP address is other than the SUP 8-E itself. This results in AP joining the MC and not the MA.

## Upgrading the System Software

For details on how to upgrade ROMMON, refer to:

[http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/release/note/OL\\_30306-01.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/release/note/OL_30306-01.html)

Follow these guidelines:

- If you are upgrading to Cisco IOS XE Release 3.8.1E and using Supervisor Engine 8L-E, you must upgrade to ROMMON 15.1(1r)SG6 before upgrading the IOS-XE image to 3.8.1E or newer versions.
- If you are upgrading to Cisco IOS XE Release 3.8.xE and plan to use VSS, you must upgrade your ROMMON to version 15.0(1r)SG10. Otherwise, you must upgrade your ROMMON to at least Version 15.0(1r)SG2.
- If you are upgrading to Cisco IOS XE Release 3.8.xE and using Supervisor Engine 7-E or 7L-E, you must use ROMMON version 15.0(1r)SG10 or a higher version (if available).
- If you are upgrading to Cisco IOS XE Release 3.8.0E and using Supervisor Engine 8-E, you must use ROMMON version 15.1(1r) SG5 or later, version or a higher version (if available).




---

**Note** If dual supervisor engines are present, first upgrade your software to Cisco IOS XE 3.2.0SG or higher, then upgrade your ROMMON to version 15.0(1r)SG7 to avoid an uplinks issue (CSCtj54375).

---

## Manual Field Programmable Gate Array Upgrades

If you have installed WS-X4748-UPOE in the chassis, note the following:

With Cisco IOS XE Release 3.8.xE, after an ISSU upgrade, you may have to manually upgrade the Field Programmable Gate Array (FPGA) for WS-X4748-UPOE+E line cards that have version ID (VID) 03 or later versions. (To check the VID, enter the show inventory command in privileged EXEC mode).

The required FPGA upgrades are not triggered automatically after an ISSU upgrade. This may result in an unexpected FPGA upgrade of all applicable linecards if a linecard is inserted online (OIR), after ISSU upgrade. The solution to this problem is to manually perform an FPGA upgrade during a maintenance window.

Follow these steps for all WS-X4748-UPOE+E linecards in the chassis:

```
Switch(config)# service internal
Switch(config)# end
Switch# hw-module module-number upgrade-fpga-all
```



## Identifying Hardware Revisions on the Switch Chassis

The hardware revision is a number that represents a hardware upgrade. Enter the **show idprom chassis** privileged EXEC command on the switch chassis to know its current revision number.

Some chassis require a certain hardware revision to be operable with certain devices. For example, the Cisco Catalyst 4507R-E Switch chassis must have hardware revision 2.0 or higher to support Supervisor Engine 8-E or 8L-E. Before you install Supervisor Engine 8-E or 8L-E on the Catalyst 4507R-E Switch chassis, verify that the chassis has the required revision number.

The following is a sample output of the **show idprom chassis** command on a Catalyst 4507R-E Switch. Note the “Hardware Revision” field here is “2.0”:

```
Switch# show idprom chassis
Chassis Idprom :
  Common Block Signature = 0xABAB
  Common Block Version = 3
  Common Block Length = 144
  Common Block Checksum = 3874
  Idprom Size = 256
  Block Count = 4
  FRU Major Type = 0x4001
  FRU Minor Type = 52
  OEM String = Cisco
  Product Number = WS-C4507R-E
  Serial Number = FOX1224G5ZH
  Part Number = 73-9975-04
  Part Revision = D0
  Manufacturing Deviation String =
Hardware Revision = 2.0
  Top Assembly Number = 800-26494-01
  Top Assembly Revision Number = D0
<output truncated>
```

## Upgrading ROMMON Image for Supervisor Engine 8-E

For IOS XE 3.8.xE, the ROMMON image must be upgraded to use version 15.1(1r)SG5. The IOS XE Bundle format for Supervisor Engine 8-E has changed, necessitating a new ROMMON image.

The following [error] messages might be observed if IOS XE 3.7.xE images are booted with older ROMMON images:

```
rommon 1 > boot bootflash:cat4500es8-universalk9.SPA.03.06.00.E.152-2.E.bin
File has bad file magic number: 0x0. Is it a valid file?
boot: cannot load "bootflash:cat4500es8-universalk9.SPA.03.06.00.E.152-2.E.bin?;

rommon 10 > boot tftp://172.18.121.121/cat4500es8-universalk9.SPA.03.06.00.E.152-2.E.bin
Link Speed : 100Mb Full Duplex
Filename : /cat4500es8-universalk9.SPA.03.06.00.E.152-2.E.bin
IpAddress : 10.122.161.35
TftpServer : 172.18.121.121
TftpBlkSize : 1468
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File Size : 199051336
MD5 : a32df24fdfc54776f20d83c092f24496

Unsigned image, or verification is disabled!
Image Error!!!!
```

## Identifying an +E Chassis and ROMMON

When supervisor engine 1 (sup1) is in ROMMON and supervisor engine 2 (sup2) is in IOS, only sup2 can read the idprom contents of chassis' idprom. Chassis type is displayed as "+E" in the output of the **show version** command. Conversely, sup1 can only display the chassis type as "E."

When both sup1 and sup2 are in ROMMON, both engines can read the chassis' idprom. Chassis type is displayed correctly as "+E" in the output of the **show version** command.

When both sup1 and sup2 are in IOS, both engines can read the chassis' idprom. Chassis type is displayed correctly as "+E" in the output of the **show version** command.

## Limitations and Restrictions

- For few ACLs, OGACL programming results in "Partial Programmed" state. (CSCvc21299)
- 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 crash. As a workaround, disable the logging discriminator on the device (CSCur45606, CSCur28336)
- If WLAN applied client policy is invalid, the client is excluded with the exclusion reason being 'Client QoS Policy failure'.
- The maximum MTE supported on Catalyst 4500 switches is 8000, per direction.
- Although the **show memory** command is supported on Catalyst 4500 series switches, the CLI output for the command shows the value 0 for config total, on Catalyst 4500 series switches using a daughter card on Supervisor Engine 7-E. This issue is, however, not seen on switches with Supervisor Engine 7-E baseboard. (CSCup28930)
- The system allows you to delete policy maps related to these Auto QoS profiles:
  - Auto QoS enterprise
  - Auto QoS guest
  - Auto QoS voice

The problem is seen on a Catalyst 4500 series switch running Cisco IOS-XE release 3.7.0E, when you configure QoS using Auto Qos and you try to delete an Auto QoS profile related policy map.

**Workaround:** To recover the deleted policy-map, remove all the policies related to that profile, remove Auto QoS configuration from the WLAN, and then reconfigure Auto QoS.

- Dot1x PEAP based authentication for wireless clients on Supervisor Engine 8-E is 3 auths/sec.
- Indirectly connected access points are not supported. Only access points directly connected to a trunk or access port is supported. On connecting more than one AP the following error message will be seen:
 

```
3.Dec 5 03:57:24.121: %CAPWAP-3-ONE_AP_PER_PORT: AP (mac:6c20.56a6.4fc4) is not
allowed on port:Po2. Only one AP per port is allowed.
```
- RPR mode cannot be configured when Supervisor Engine 8-E is booted in wireless mode.
- Flow Sampling is not supported on Supervisor Engine 8-E.

- Supported QoS features on wireless targets: The detailed QoS policy is the same as mentioned here: [http://www.cisco.com/c/en/us/td/docs/wireless/controller/5700/software/release/3e/qos/configuration\\_guide/b\\_qos\\_3e\\_5700\\_cg/b\\_qos\\_3e\\_5700\\_cg\\_chapter\\_011.html#concept\\_47CC8E2ACA2E44489B9BB7068FCD0649](http://www.cisco.com/c/en/us/td/docs/wireless/controller/5700/software/release/3e/qos/configuration_guide/b_qos_3e_5700_cg/b_qos_3e_5700_cg_chapter_011.html#concept_47CC8E2ACA2E44489B9BB7068FCD0649)), except that the port policy cannot be changed because it is a DC-interconnect port.
- VSS: Do not use SVLAN for routing in SP network on ingress switch (where the mapping is present). This is not a valid scenario.
- VSS is not supported in Wireless mode, on Supervisor Engine 8-E.
- Wired guest access does not work on Supervisor Engine 8-E, in multi-host or multi-authentication mode.
- The **show exception files all** command lists only crashinfo files from the active supervisor engine. You must issue the **dir slavecrashinfo:** and **dir slavecrashinfo-dc:** commands to obtain lists of crashinfo files from the standby supervisor engine.
- Performing an ISSU from a prior release to IOS XE 3.6.0E is not supported.
- The WS-X4712-SFP+E module is not supported in the WS-C4507R-E or WS-C4510R-E chassis and does not boot. This module is supported in the WS-C4503-E, WS-C4506-E, WS-C4507R+E, and WS-C4510R+E chassis.
- More than 16K QoS policies can be configured in software. Only the first 16K are installed in hardware.
- Adjacency learning (through ARP response frames) is restricted to roughly 1000 new adjacencies per second, depending on CPU utilization. This should only impact large networks on the first bootup. After adjacencies are learned they are installed in hardware.
- Multicast fastdrop entries are not created when RPF failure occurs with IPv6 multicast traffic. In a topology where reverse path check failure occurs with IPv6 multicast, this may cause high CPU utilization on the switch.
- The SNMP ceImageFeature object returns a similar feature list for all the three license levels (LAN Base, IP Base, and EntServices). Although the activated feature set for a universal image varies based on the installed feature license, the value displayed by this object is fixed and is not based on the feature license level.
- Standard TFTP implementation limits the maximum size of a file that can be transferred to 32 MB. If ROMMON is used to boot an IOS image that is larger than 32 MB, the TFTP transfer fails at the 65,xxx datagram.

TFTP numbers its datagrams with a 16 bit field, resulting in a maximum of 65,536 datagrams. Because each TFTP datagram is 512 bytes long, the maximum transferable file is  $65536 \times 512 = 32$  MB. If both the TFTP client (ROMMON) and the TFTP server support block number wraparound, no size limitation exists.

Cisco has modified the TFTP client to support block number wraparound. So, if you encounter a transfer failure, use a TFTP server that supports TFTP block number wraparound. Because most implementations of TFTP support block number wraparound, updating the TFTP daemon should fix the issue.

- A XML-PI specification file entry does not return the desired CLI output.

The outputs of certain commands, such as **show ip route** and **show access-lists**, contain non-deterministic text. While the output is easily understood, the output text does not contain strings that are consistently output. A general purpose specification file entry is unable to parse all possible output.

#### Workaround (1):

While a general purpose specification file entry may not be possible, a specification file entry might be created that returns the desired text by searching for text that is guaranteed to be in the output. If a string is guaranteed to be in the output, it can be used for parsing.

For example, the output of the **show ip access-lists SecWiz\_Gi3\_17\_out\_ip** command is this:

```
Extended IP access list SecWiz_Gi3_17_out_ip
 10 deny ip 76.0.0.0 0.255.255.255 host 65.65.66.67
 20 deny ip 76.0.0.0 0.255.255.255 host 44.45.46.47
 30 permit ip 76.0.0.0 0.255.255.255 host 55.56.57.57
```

The first line is easily parsed because access list is guaranteed to be in the output:

```
<Property name="access list" alias="Name" distance="1.0" length="-1" type="String" />
```

The remaining lines all contain the term host. As a result, the specification file may report the desired values by specifying that string. For example, this line

```
<Property name="host" alias="rule" distance="s.1" length="1" type="String" />
```

will produce the following for the first and second rules

```
<rule>
  deny
</rule>
```

and the following for the third statement

```
<rule>
  permit
</rule>
```

**Workaround (2):**

Request the output of the **show running-config** command using NETCONF and parse that output for the desired strings. This is useful when the desired lines contain nothing in common. For example, the rules in this access list do not contain a common string and the order (three permits, then a deny, then another permit), prevent the spec file entry from using permit as a search string, as in the following example:

```
Extended MAC access list MACCOY
 permit 0000.0000.ffef ffff.ffff.0000 0000.00af.bcef ffff.ff00.0000 appletalk
 permit any host 65de.edfe.fefe xns-idp
 permit any any protocol-family rarp-non-ipv4
 deny host 005e.1e5d.9f7d host 3399.e3e1.ff2c dec-spanning
 permit any any
```

The XML output of **show running-config** command includes the following, which can then be parsed programmatically, as desired:

```
<mac><access-list><extended><ACLName>MACCOY</ACLName></extended></access-list></mac>
 <X-Interface> permit 0000.0000.ffef ffff.ffff.0000 0000.00af.bcef ffff.ff00.0000
 appletalk</X-Interface>
 <X-Interface> permit any host 65de.edfe.fefe xns-idp</X-Interface>
 <X-Interface> permit any any protocol-family rarp-non-ipv4</X-Interface>
 <X-Interface> deny host 005e.1e5d.9f7d host 3399.e3e1.ff2c
 dec-spanning</X-Interface>
 <X-Interface> permit any any</X-Interface>
```

**CSCtg93278**

- When attaching a existing policy-map (that is already applied to a control-port) to another front-panel port, the following message displays:

The `polycymap <policy-map name>` is already attached to control-plane and cannot be shared with other targets.

**Workaround:** Define a policy-map with a different name and then reattach. CSCti26172

- If the number of unique FNF monitors attached to target exceeds 2048 (one per target), a switch responds slowly:

**Workarounds:**

- Decrease the number of monitors.
- Attach the same monitor to multiple targets. CSCti43798

- **ciscoFlashPartitionFileCount** object returns an incorrect file count for **bootflash:**, **usb0:**, **slot0:**, **slaveslot0:**, **slavebootflash:**, and **slaveusb0:**.

**Workaround:** Use the `dir device` command (for example, `dir bootflash:`) to obtain the correct file count. CSCti74130

- If multicast is configured and you make changes to the configuration, Traceback and CPUHOG messages are displayed if the following conditions exist:

- At least 10K groups and roughly 20K mroutes exist.
- IGMP joins with source traffic transit to all the multicast groups.

This is caused by the large number of updates generating SPI messages that must be processed by the CPU to ensure that the platform is updated with the changes in all the entries.

**Workaround:** None. CSCti20312

- With traffic running, entering **clear ip mroute \*** with larger number of mroutes and over 6 OIFs will cause Malloc Fail messages to display.

You cannot clear a large number of mroutes at one time when traffic is still running.

**Workaround:** Do not clear all mroutes at once.

CSCtn06753

- Although you can configure subsecond PIM query intervals on Catalyst 4500 platforms, such an action represents a compromise between convergence (reaction time) and a number of other factors (number of mroutes, base line of CPU utilization, CPU speed, processing overhead per 1 m-route, etc.). You must account for those factors when configuring subsecond PIM timers. We recommend that you set the PIM query interval to a minimum of 2 seconds. By adjusting the available parameters, you can achieve flawless operation; that is, a top number of multicast routes per given convergence time on a specific setup.
- Energywise WOL is not “waking up” a PC in hibernate or standby mode.

**Workaround:** None. CSCtr51014

- The ROMMON version number column in the output of **show module** command is truncated.

**Workaround:** Use the **show version** command. CSCtr30294

- IP SLA session creation fails randomly for various 4-tuples.

**Workaround:** Select an alternate destination or source port. CSCty05405

- The system cannot scale to greater than 512 SIP flows with MSP and metadata enabled.

**Workaround:** None. CSCty79236

- On the following linecards running IOS XE Release 3.2.3:

- 10/100/1000BaseT Premium POE E Series WS-X4648-RJ45V+E (JAE1348OY52)

- 4 Sup 7-E 10GE (SFP+), 1000BaseX (SFP) WS-X45-SUP7-E (CAT1434L0G4)

the following restrictions apply:

- Sub-interfaces are not supported on 1 Gigabit and Ten-Gigabit interfaces.
- Port-channel members do not support multiple classification criteria for a QoS policy.
- CEF is disabled automatically when uRFP is enabled and TCAM is fully utilized.
- When either the RADIUS-server test feature is enabled or RADIUS-server dead-criteria is configured, and either RADIUS-server deadtime is set to 0 or not configured, the RADIUS-server status is not properly relayed to AAA.

**Workaround:** Configure both dead-criteria and deadtime.

```
radius-server dead-criteria
radius-server deadtime
```

CSCtl06706

- If you use the **quick** option in the **issu changeversion** command, the following might occur:
  - Links flap for various Layer 3 protocols.
  - A traffic loss of several seconds is observed during the upgrade process.

**Workaround:** Do not use the **quick** option with the **issu changeversion** command. CSCto51562

- While configuring an IPv6 access-list, if you specify **hardware statistics** as the first statement in v6 access-list mode (i.e. before issuing any other v6 ACE statement), it will not take effect. Similarly, your hardware statistics configuration will be missing from the output of the **show running** command.

You will not experience this behavior with IPv4 access lists.

**Workaround:** During IPv6 access-list configuration, configure at least one IPv6 ACE before the "hardware statistics" statement. CSCuc53234

- Routed packets that are fragmented are not policed if the egress interface is on the VSS Standby switch. However, if the egress interface is on the VSS Active switch, these packets are policed. This applies to QoS policing only. QoS marking, shaping and sharing behave as expected.

**Workaround:** None. CSCub14402

- When an IPv6 FHS policy is applied on a VLAN and an EtherChannel port is part of that VLAN, packets received by EtherChannel (from neighbors) are not bridged across the local switch.

**Workaround:** Apply FHS policies on a non EtherChannel port rather than a VLAN. CSCua53148

- During VSS conversion, the switch intended as the Standby device may require up to 9 minutes to reach an SSO state. The boot up time depends on the configuration and on the number of line cards in the system.

**Workaround:** None. CSCua87538

- Dual connectors (like, an SFP+ transceiver inserted into a CVR-X2-SFP10G module) on the WS-X4606-X2-E line card are not supported as a VSL.

**Workaround:** Use any X2-pluggable module on its own in the WS-X4606-X2-E line card. CSCuc70321

- Memory allocation failures can occur if more than 16K IPv6 multicast snooping entries are present.

**Workaround:** None. CSCuc77376

- The **show interface capabilities** command output does not show the correct linecard model.

**Workaround:** Observe the **show module** command output. CSCua79513

- Beginning with IOS Release XE 3.5.0E, error messages that occur when a QoS policy is applied will no longer appear directly on the console when **no logging console** is configured. They will appear only when a logging method is active (e.g., logging buffered, logging console, ...).

**Workaround:** None. CSCuf86375

- Setting a cos value based on QoS group triggers the following error message in a VSS system
- ```
set action fail = 9
```

**Workaround:** None. QoS groups are not supported in VSS. CSCuc84739

- Auto negotiation cannot be disabled on the Fa1 port. It must be set to auto/auto, or fixed speed with duplex auto.
- The following messages are seen during boot up after POST check.

```
Rommon reg: 0x00004F80
Reset2Reg: 0x00000F00

Image load status: 0x00000000
#####
Snowtrooper 220 controller 0x0430006E..0x044E161D Size:0x0057B4C5 Program Done!
#####
[ 6642.974087] pci 0000:00:00.0: ignoring class b20 (doesn't match header type 01)
Starting System Services
Calculating module dependencies ...
Loading rtc-ds1307
RTNETLINK answers: Invalid argument
No Mountpoints DefinedJan 17 09:48:14 %IOSXE-3-PLATFORM: process sshd[5241]: error:
Bind to port

22 on :: failed: Address already in use
Starting IOS Services
Loading virtuclock as vuclock
Loading gsbu64atomic as gdb64atomic
/dev/fd/12: line 267: /sys/devices/system/edac/mc/edac_mc_log_ce: No such file or
directory
Aug 8 20:30:29 %IOSXE-3-PLATFORM: process kernel: mmc0: Got command interrupt
0x00030000 even though no command operation was in progress.

Aug 8 20:30:29 %IOSXE-3-PLATFORM: process kernel: PME2: fsl_pme2_db_init: not on
ctrl-plane
```

These messages are cosmetic only, and no ssh services are available unless configured within IOS.

**Workaround:** None CSCue15724

## 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](#)
- [Open Caveats for Cisco IOS XE Release 3.8.xE](#)
- [Resolved Caveats in Cisco IOS XE Release 3.8.9E](#)
- [Resolved Caveats in Cisco IOS XE Release 3.8.8E](#)
- [Resolved Caveats in Cisco IOS XE Release 3.8.7E](#)

- [Resolved Caveats in Cisco IOS XE Release 3.8.6E](#)
- [Resolved Caveats for Cisco IOS XE Release 3.8.5aE](#)
- [Resolved Caveats for Cisco IOS XE Release 3.8.5E](#)
- [Resolved Caveats for Cisco IOS XE Release 3.8.4E](#)
- [Resolved Caveats in Cisco IOS XE Release 3.8.3E](#)
- [Resolved Caveats in Cisco IOS XE Release 3.8.2E](#)
- [Resolved Caveats for Cisco IOS XE Release 3.8.1E](#)
- [Resolved Caveats for Cisco IOS XE Release 3.8.0E](#)

**Note**

For the latest information on PSIRTS, refer to the Security Advisories on CCO at the following URL:

[http://www.cisco.com/en/US/products/products\\_security\\_advisories\\_listing.html](http://www.cisco.com/en/US/products/products_security_advisories_listing.html)

## Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The 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 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 listed in this document:

1. Access the BST (use your Cisco user ID and password) at <https://tools.cisco.com/bugsearch/>.
2. Enter the bug ID in the **Search For:** field.



## Open Caveats for Cisco IOS XE Release 3.8.xE

Use the Bug Search Tool to view the details of a caveat listed in this section:

| Bug ID                     | Headline                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| <a href="#">CSCva26201</a> | 3750X is not sending correct DSCP value in cflow IP header.                                         |
| <a href="#">CSCvk21769</a> | C2960L packet loss on 10M/Full port.                                                                |
| <a href="#">CSCvk38377</a> | C4K_SNIPSMAN-3-GTXRXRESETFAILURE: Gtx Rx Reset Error in Snips.                                      |
| <a href="#">CSCvm36476</a> | C2960 plus handling GARP unexpectedly.                                                              |
| <a href="#">CSCvm24330</a> | Tracebacks seen on loadversion due to MTU mismatch.                                                 |
| <a href="#">CSCvo24813</a> | WS-C4510R+E / Dual WS-X45-SUP8-E / Crash when configuring flow exporter                             |
| <a href="#">CSCvo37003</a> | C4500 not showing MAC add of device (Avaya phone) in "show mac add" table after enabling mab,dot1x. |
| <a href="#">CSCvo38680</a> | C6800IA-48FPD (FEX) reloads with a last reload reason of "Unknown reason".                          |

## Resolved Caveats in Cisco IOS XE Release 3.8.9E

| Bug ID                     | Headline                                                                                        |
|----------------------------|-------------------------------------------------------------------------------------------------|
| <a href="#">CSCut66603</a> | Device stuck on 4500X VSS during Rommon version upgrade                                         |
| <a href="#">CSCvd67904</a> | 4500X does not run dot1x when a laptop wakes from sleep mode                                    |
| <a href="#">CSCvk74432</a> | AFTER ADDING NEW VLAN IN REP SEGMENT THERE IS A LAYER 2 LOOP                                    |
| <a href="#">CSCvn72973</a> | Device is getting crashed on the "cts role-based enforcement"                                   |
| <a href="#">CSCuv90519</a> | IKEv2 session fails to come up after tunnel source address change                               |
| <a href="#">CSCve21224</a> | ewlc: wncd crash seen at auth_mgr_pre_shim_handle_pre_event                                     |
| <a href="#">CSCve57810</a> | Device failing over without 'fail next-method' or 'no-response next method'                     |
| <a href="#">CSCvj23301</a> | IOS: Crypto Ruleset fails to get deleted                                                        |
| <a href="#">CSCvk56331</a> | Initial contact in IKEv1 phase 2 rekey (QM1) causes all crypto sessions to drop                 |
| <a href="#">CSCvn13735</a> | Failure to detect the back to back CoA requests, leading to policy deletion.                    |
| <a href="#">CSCvn00129</a> | After CoA push from ISE, Result of "show cts policy sgt" has multiple policies for "to unknown" |
| <a href="#">CSCvp76403</a> | Defaulting interface config on dot1x interface results in incorrect port-control state on port  |

## Resolved Caveats in Cisco IOS XE Release 3.8.8E

| Bug ID                     | Headline                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvc71220</a> | Fix the quotes issue in SA build infra                                                             |
| <a href="#">CSCve89361</a> | Crash in SISF while processing IPv6 packet                                                         |
| <a href="#">CSCvf70676</a> | Interface flaps on 4724-SFP/4748-SFP module with 100M SFP GLC-GE-100FX                             |
| <a href="#">CSCvj86626</a> | Clients stuck in authentication loop when interface template is pushed from Radius server          |
| <a href="#">CSCvk44790</a> | WS-X45-SUP7-E with MMU and preemption not effective upon fail back to active                       |
| <a href="#">CSCvk62735</a> | 3750   high CPU   HAACL Acl Manager                                                                |
| <a href="#">CSCvm21098</a> | OSPFv3 BFD is broken                                                                               |
| <a href="#">CSCvm43071</a> | [IBNS 2.0] aaa-available event is not being triggered when using authentication/authorization list |
| <a href="#">CSCvm52157</a> | Cat4K/sup8-E VSS 3.8.5aE- running out of CPU and IO memory resources while clearing access-session |
| <a href="#">CSCvm87280</a> | %C4K_CHASSIS-3-ALLMODULETEMPERATURESENSORSFAILED shows randomly when we removal/insertion          |
| <a href="#">CSCvm90630</a> | 4500 forwards traffic on BKN interface                                                             |
| <a href="#">CSCvm96180</a> | Cat4500 switch reboots unexpectedly after certain Netflow configuration is pushed via SSH          |

|                            |                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------|
| <a href="#">CSCvn18256</a> | "platform" command on VSS gets switch on a boot loop                                     |
| <a href="#">CSCvo08913</a> | can't issu from 3.8.6E to 3.10.2E due to an inconsistency between the Active and Standby |

## Resolved Caveats in Cisco IOS XE Release 3.8.7E

**Table 20** *Resolved Caveats in Cisco IOS XE Release 3.8.7E*

| <b>Bug ID</b>              | <b>Headline</b>                                                                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------|
| <a href="#">CSCva10393</a> | System crashed during boot up on 4948E.                                                                       |
| <a href="#">CSCvd87317</a> | The <b>ip access-list logging hash-generation</b> command not function expectedly.                            |
| <a href="#">CSCve37498</a> | Switch sends duplicate accounting message, that causing ISE to generate misconfigured NAS Alarms.             |
| <a href="#">CSCve69049</a> | Crash when it tries to write over a TTY session.                                                              |
| <a href="#">CSCve73467</a> | Link not up on M-gig line cards WS-X4748-12X48U+E with cable length of 300Ft.                                 |
| <a href="#">CSCvg82674</a> | VSS Standby crashes @ /k5/aclman/K5AclProfileMapEntry.cxx:135                                                 |
| <a href="#">CSCvh28285</a> | H/W mac address table learn wrong mac address on C4500X VSS with Flexlink switchover.                         |
| <a href="#">CSCvh79168</a> | Crash on numPolicersPerBank with Invalid policerBaseIndex.                                                    |
| <a href="#">CSCvh89534</a> | 4500 Sup 8E DACL applied to the incorrect interface.                                                          |
| <a href="#">CSCvi01706</a> | Removing ACE from long ACL interrupts traffic.                                                                |
| <a href="#">CSCvi25365</a> | 2960x - session to the member switch fails in stack.                                                          |
| <a href="#">CSCvi50136</a> | Repeated Modification of ACL causes standby switch to crash.                                                  |
| <a href="#">CSCvj29126</a> | RADIUS client on network fails to solicit PAC key from Cisco TrustSec even though the device has a valid PAC. |
| <a href="#">CSCvj41439</a> | ACL TCAM USAGE is different when using the same ACL configuration but different IOS version.                  |
| <a href="#">CSCvk23596</a> | Additional fix needed for CSCvg34881 (Catalyst 4500 crash when WS-X4748 card goes down).                      |
| <a href="#">CSCvk52487</a> | 3750X Switch crash due to memory leak in HL2MCM process.                                                      |
| <a href="#">CSCvi06070</a> | OSPF and BGP keeps flapping every few seconds when BFD is enabled on Catalyst 4000 device                     |

## Resolved Caveats in Cisco IOS XE Release 3.8.6E

| Bug ID                     | Headline                                                                                                        |
|----------------------------|-----------------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvb43407</a> | 10G LRM SFPs getting Unsupported error logs in sup8le uplinks.                                                  |
| <a href="#">CSCvc40729</a> | Cisco IOS and IOS XE Software Bidirectional Forwarding Detection Denial of Service Vulnerability.               |
| <a href="#">CSCvd40673</a> | Cisco Smart Install Denial of Service Vulnerability.                                                            |
| <a href="#">CSCve05543</a> | Interface not coming up if replace GLC-T/100M to Fiber SFP.                                                     |
| <a href="#">CSCve91257</a> | Catalyst 4000 Series Switches crash with FlatAclMan.                                                            |
| <a href="#">CSCvf46500</a> | VSL Port-Channel in W state after OIR.                                                                          |
| <a href="#">CSCvf70676</a> | Interface flaps on 4724-SFP/4748-SFP module with 100M SFP GLC-GE-100FX                                          |
| <a href="#">CSCvf96579</a> | Catalyst 2960 Series Switches: AAA Radius authentication fails with <b>switchport voice vlan dot1p</b> command. |
| <a href="#">CSCvg34881</a> | Catalyst 4500 Supervisor Crashes When Turning Off LED on Failed WS-X4748 Card.                                  |
| <a href="#">CSCvg70852</a> | Unknown MAC addresses appear on port when trying to authenticate using dot1x.                                   |
| <a href="#">CSCvg74926</a> | Catalyst 4510 Sup 8 sending invalid LACP mac-ID, generates MULTIPLE_NEIGHBORS upstream.                         |
| <a href="#">CSCvg97016</a> | Memory Leak with IPDT [IP Device Tracking].                                                                     |
| <a href="#">CSCvh04891</a> | VSS Switch crash at boot time when CR (i.e. 'r') character is present in the startup-configuration.             |

## Resolved Caveats for Cisco IOS XE Release 3.8.5aE

| Bug ID                     | Headline                                         |
|----------------------------|--------------------------------------------------|
| <a href="#">CSCvg42682</a> | Key reinstallation attacks against WPA protocol. |

## Resolved Caveats for Cisco IOS XE Release 3.8.5E

| Bug ID                     | Headline                                                                                                  |
|----------------------------|-----------------------------------------------------------------------------------------------------------|
| <a href="#">CSCva86436</a> | No export IPv4 unicast map triggered router to crash.                                                     |
| <a href="#">CSCvc72751</a> | Endpoint bypasses restriction given by ISE and gets network access.                                       |
| <a href="#">CSCuz61109</a> | Self ping to port channel subinterface dropped with LISP decap log.                                       |
| <a href="#">CSCuz94245</a> | IGP-LDP sync interoperability for OSPF multiarea adjacency.                                               |
| <a href="#">CSCuz95753</a> | Paramiko SSH client, having password authentication, fails to connect to IOS.                             |
| <a href="#">CSCve31797</a> | Make toggling Cisco TrustSec SGACL enforcement on Port-channel consistent with other Cisco TrustSec CLIs. |
| <a href="#">CSCva86436</a> | No export IPv4 unicast map triggered router to crash.                                                     |

## Resolved Caveats for Cisco IOS XE Release 3.8.4E

Use the Bug Search Tool to view the details of a caveat listed in this section:

| Bug ID                     | Headline                                                                    |
|----------------------------|-----------------------------------------------------------------------------|
| <a href="#">CSCun71347</a> | 3850 Crash in "CEF: IPv4" Process While Processing ARP Throttle Elements    |
| <a href="#">CSCux05246</a> | snmpwalk and snmpget have incorrect behavior on IP SLA                      |
| <a href="#">CSCuz28618</a> | sup2t: sup crashed after MFIB errors                                        |
| <a href="#">CSCuz57145</a> | when QinQ is used DSCP values are being erased                              |
| <a href="#">CSCva21378</a> | %DTLS-3-PKI_ERROR: 6 wcm: & *%CAPWAP-3-DTLS_CONN_ERR on ISSU.               |
| <a href="#">CSCva45821</a> | IOS switch does not update native VLAN in LLDP                              |
| <a href="#">CSCvb04162</a> | 4500 IPv6 QoS Policy w/ L4Ops Intermittently Not Installing on Interface    |
| <a href="#">CSCvb11798</a> | 4500 frequent reload and High CPU due to Acl-Flattener                      |
| <a href="#">CSCvb43870</a> | When 10gSR & Zr SFPs inserted in sup8LE uplink port state are fluctuates    |
| <a href="#">CSCvb47673</a> | SYS-2-MALLOCFAIL- Traceback and Crash observed in 2k stack                  |
| <a href="#">CSCvb64236</a> | Not able to run ip redirects after deleted the secondary IP address         |
| <a href="#">CSCvb76862</a> | 4500VSS: Traffic Dropped on VSL due to SPTDROP                              |
| <a href="#">CSCvb78700</a> | Unknown unicast floodset broken                                             |
| <a href="#">CSCvb84286</a> | Jumbo CDP frames dropped / not handled by CPU when received on port-channel |

|                            |                                                                        |
|----------------------------|------------------------------------------------------------------------|
| <a href="#">CSCvb91425</a> | Output drops increased after enabling PIM on VLAN                      |
| <a href="#">CSCvb98872</a> | %SPANTREE-2-RECV_PVID_ERR: detected if new vlan created                |
| <a href="#">CSCvc03727</a> | IPDT host tracking max limit doesn't work correctly                    |
| <a href="#">CSCvc16761</a> | Switch silently dropping ARP on TenGig interface                       |
| <a href="#">CSCvc20156</a> | Repeated VfeTqBuffersUsedUnderrun interrupts cause a switch reload     |
| <a href="#">CSCvc21299</a> | OGACL:30K IN and OUT ACEs scale Partially Programmed                   |
| <a href="#">CSCvc84352</a> | IP Phone connectivity loss with dynamically assigned vlan and MDA      |
| <a href="#">CSCvc95996</a> | cauverymr4:snmp reports wrong switch numbers in ciscoEnvMonSupplyState |

## Resolved Caveats in Cisco IOS XE Release 3.8.3E

Use the Bug Search Tool to view the details of a caveat listed in this section:

**Table 21** *Resolved Caveats in Cisco IOS XE Release 3.8.3E*

| Bug ID                     | Headline                                                                                                                                |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">CSCuz42775</a> | Cat4500: PoE devices not granted power by WS-X4748-UPOE module                                                                          |
| <a href="#">CSCuv15017</a> | VSS Active Reload causes CTS Ether-channel links on standby to flap.                                                                    |
| <a href="#">CSCux91543</a> | IOSd reloads unexpectedly with daughter card failure.                                                                                   |
| <a href="#">CSCuw93750</a> | ACL merge not happening correctly in WCCP feature.                                                                                      |
| <a href="#">CSCuv68986</a> | Mobility tunnel over L3 interface on stand-by not coming up.                                                                            |
| <a href="#">CSCuw10936</a> | Cisco Catalyst 4500 Series Switch: APs not rejoining the Cisco Virtual Switching System after SSO is DTLS enabled.                      |
| <a href="#">CSCus68182</a> | 15.2(3)E2:IPDT Entries are not getting learned on portchannel.                                                                          |
| <a href="#">CSCuu21997</a> | BOOTP Reply packets flooded when wireless module is installed on Cisco Catalyst 4500E Supervisor 8-E.                                   |
| <a href="#">CSCuz59601</a> | 15.2(4)E2: 3560-CX Flash Inaccessible.                                                                                                  |
| <a href="#">CSCuv64531</a> | 3560x default G port's speed auto negotiate to 100M/bps.                                                                                |
| <a href="#">CSCva37519</a> | Stale flowmgr entry during an IPv6 Terminal Access Controller Access Control System (TACACS) transaction leads to an unexpected reload. |
| <a href="#">CSCvb24396</a> | ACL is partially programmed to hardware with the scale of IPv4 and IPv6 ACLs.                                                           |
| <a href="#">CSCvb20355</a> | Unexpected reload happens when saving configuration files greater than nonvolatile RAM (NVRAM) space.                                   |

## Resolved Caveats in Cisco IOS XE Release 3.8.2E

| Bug ID                     | Headline                                                  |
|----------------------------|-----------------------------------------------------------|
| <a href="#">CSCuy05126</a> | ISSU:Sup8-E wireless ISSU failed with rolled back to RPR. |

|                            |                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">CSCur64110</a> | Queue-based Transmit/Drop QoS counters for Cisco Catalyst 4000 Series Switches.                                                 |
| <a href="#">CSCuu66503</a> | IOS HTTPS client not enforcing subject-name verification.                                                                       |
| <a href="#">CSCUv27265</a> | ENH: Enable support for TLSv1.1 & TLSv1.2 for HTTP secure server/client.                                                        |
| <a href="#">CSCUv41355</a> | Unable to telnet: No wild listener: port 23.                                                                                    |
| <a href="#">CSCUv92875</a> | Add prefix information in IPv6 RA when system/ SVI is shutdown.                                                                 |
| <a href="#">CSCUw36080</a> | SNMP with extended ACL.                                                                                                         |
| <a href="#">CSCUw48118</a> | Cisco ASR 920 Series switches: crash in bcopy called from addnew during reassembly.                                             |
| <a href="#">CSCUw49406</a> | “no ip routing protocol purge interface” delete with reload                                                                     |
| <a href="#">CSCUx26097</a> | Debug logging - parser issue.                                                                                                   |
| <a href="#">CSCUx38417</a> | Cisco IOS and IOS-XE IKEv2 fragmentation DoS.                                                                                   |
| <a href="#">CSCUx85039</a> | Cisco Catalyst 3650 and 3850 Series Switches: Syslog produces no output when set to logging queue-limit X.                      |
| <a href="#">CSCUx99025</a> | Evaluation of Cisco IOS and IOS-XE1 for NTP January 2016.                                                                       |
| <a href="#">CSCUx99594</a> | EEM policies may not be able to send emails.                                                                                    |
| <a href="#">CSCUy03680</a> | V3Lite IGMP packets sent instead of V3 when UDP based feature is present.                                                       |
| <a href="#">CSCUy05927</a> | IPC-WATERMARK and CHKPT-5-HIGHBUFFER logs leading to reload.                                                                    |
| <a href="#">CSCUy12271</a> | Wrong LSP size calculation following MAC move with OTV.                                                                         |
| <a href="#">CSCUy43392</a> | Cisco 5760 Wireless LAN Controller crash at snmp_subagent.                                                                      |
| <a href="#">CSCUy44377</a> | Syslog: Source-Interface address change does not take effect in IPv6.                                                           |
| <a href="#">CSCUy87667</a> | Crash due to block overrun by AAA banner.                                                                                       |
| <a href="#">CSCUy92281</a> | VLAN 1 interface is shutdown during bootup.                                                                                     |
| <a href="#">CSCuz52528</a> | Evaluation of all for OpenSSL May 2016.                                                                                         |
| <a href="#">CSCUv74938</a> | Memory leak in ffm process.                                                                                                     |
| <a href="#">CSCuz02766</a> | Crash in IOSd with ‘EPC SM Liaison Update proc’.                                                                                |
| <a href="#">CSCuz13878</a> | Crash when remotely executing show license right-to-use summary.                                                                |
| <a href="#">CSCuz18217</a> | SUP8E VSS active crash due to signr 11 when OIR standby SUP8E.                                                                  |
| <a href="#">CSCud37408</a> | PerfMon entries not idle timing out.                                                                                            |
| <a href="#">CSCUy58587</a> | eicored process crash from clock sync.                                                                                          |
| <a href="#">CSCUx14323</a> | Cisco IOS Release 15.2(2)E4 and XE 3.6.4E: Cisco 5760 Wireless LAN Controller flooding wrong message when max AP count exceeds. |
| <a href="#">CSCUw78795</a> | Converged Access REPLAY_ERR message showing WLAN ID as VLAN ID of the AP.                                                       |
| <a href="#">CSCUw02812</a> | Why is there a gap of 204MB (in WCM) after 23hrs with insignificant leaks.                                                      |
| <a href="#">CSCUw91603</a> | Cisco IOS Release 15.2(3)E3 and XE 3.7.3E: MCMA SPG fields addition in <b>show wireless mobility summary</b> command.           |
| <a href="#">CSCUx79913</a> | The client column in the <b>load-info</b> command is not making much sense.                                                     |

|                            |                                                                                                                              |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">CSCux02438</a> | LWA: L2 Roam: no mobility anchor sticky configured on WLAN.                                                                  |
| <a href="#">CSCux38445</a> | Cisco1850 Access Point monitor mode is showing not supported in Cisco IOS XE Release 3.7 3E and Cisco IOS Release 15.2(3)E3. |
| <a href="#">CSCuz01017</a> | GUI is not showing interference devices.                                                                                     |
| <a href="#">CSCuz35087</a> | Lobby ambassador user-name gives full GUI access Converged Access Cisco IOS XE Release 3.7.3E.                               |
| <a href="#">CSCuu41264</a> | PEM-3-WEBAUTHCLIENTNOTIFYFAIL, not found while processing callback from NSM.                                                 |
| <a href="#">CSCuw97388</a> | SNMP should allow 128 characters for ap groups description for Converged Access.                                             |

## Resolved Caveats for Cisco IOS XE Release 3.8.1E

None

## Resolved Caveats for Cisco IOS XE Release 3.8.0E

Use the Bug Search Tool to view the details of a caveat listed in this section:

**Table 22** *Resolved Caveats in Cisco IOS XE Release 3.8.0E*

| Bug ID     | Headline                                                               |
|------------|------------------------------------------------------------------------|
| CSCtx11583 | 3750X:stack:when new switch join stack, traffic loss can be seen.      |
| CSCun33897 | 4500 IOS-XE: Crash on ACL/PBR configuration                            |
| CSCup03795 | SPAN breaks on ACTIVE port after switchover in VSS setup               |
| CSCup89543 | ping with packet size 1469 fails after config span on 4500X VSS        |
| CSCuq54573 | Service Policy disappears from Running Configuration of the interface  |
| CSCuq66263 | Switch crashes when ACL add entry                                      |
| CSCur84243 | WS-X4640-CSFP-E ports (Tx) are disabled on start-up                    |
| CSCur98467 | VSL-MGMT access-list mac address changes after entire VSS reload       |
| CSCus13924 | Device crashes while configuring 'Identity' commands                   |
| CSCut04550 | Beni E1:Auth rates are too low for central webauth.                    |
| CSCut09985 | VSL link stuck in W state, when OIR is done on the SFP of the VSL link |
| CSCut54992 | HSRP duplicated packets are detected                                   |
| CSCut82734 | IOSD-EXT-SIGNAL: Segmentation fault(11), Process = Cat4k Mgmt HiPri    |
| CSCuu43197 | C4500X high CPU due to execute show command continuously               |
| CSCuu83085 | Memory leaks @ AAA Account Response.                                   |
| CSCuu89948 | upolicer action issues with mixed traffic hitting wrong action         |
| CSCuu92224 | 2960X - EPM vlan plugin crash                                          |
| CSCuv22441 | Cannot match cos in 3.7.0 Lanbase                                      |
| CSCup93935 | RRM must not push DFS channel change to all of RF group                |



**Table 22** *Resolved Caveats in Cisco IOS XE Release 3.8.0E (continued)*

| <b>Bug ID</b> | <b>Headline</b>                                                          |
|---------------|--------------------------------------------------------------------------|
| CSCur10397    | ap core-dump ip validation is wrong                                      |
| CSCur14709    | 5760 AP TCP MSS defaults to 536                                          |
| CSCur60244    | 5760 webauth on mac filter failure fails on new mobility with 5500 WLC   |
| CSCur87501    | post-ACL not applied after CWA CoA in New Mobility with 3850 as foreign  |
| CSCus49969    | NGWC - AP syslog shows with the wrong byte order                         |
| CSCus77477    | NGWC Increase the number of URLs allowed in a DNS ACL in wlc             |
| CSCut88813    | WLAN cannot be configured with a space in psk shared key on NGWC 3.7     |
| CSCuu00760    | stale IPDT entries with %WCDB-3-WCDB_IP_CONFLICT error with guest anchor |
| CSCuu12308    | CWA does not properly work with 2 anchors configured on the WLAN         |
| CSCuu14197    | AIR-CT5760-K9 WCM crash in process process_get_next                      |
| CSCuu23734    | NGWC CLI CleanAir Persistent Device Propagation help message is wrong    |
| CSCuu23858    | Persistent Device Propagation cannot be configured via GUI               |
| CSCuu29813    | DHCP snoop on uplink vlan create WCDB error, does not match binding vlan |
| CSCuu32303    | AP radio interfaces admin down state after WLC reboot                    |
| CSCuu47450    | 7925 roam will fail intermittently(client stuck in authenticating state) |
| CSCuu50589    | Voice Clients Blacklisted due to %SPI-3-QOS_INSTALL_CLIENT_POLICY        |
| CSCuu59697    | AP does not forward EAPoL-Key M1 to client when AVC is enabled           |
| CSCuu61591    | WLAN with space cannot be added to AP group                              |
| CSCuu71587    | WPA-AES config getting disabled on the CLI after WLC/switch reboot       |
| CSCuu73067    | The cmd "show ap join stats summary" outputs error message               |
| CSCuv14890    | DHCPv6 solicit frame (IPv6 multicast) frame replication issues           |
| CSCuv23751    | NGWC: 'JP' should be used as world mode in Beacon/Probe Res              |
| CSCuv69997    | 5760 crash due to APF-3-VALIDATE_DOT11i_CIPHERS_FAILED Errors            |
| CSCuu27982    | T29.13 PT can not work well on Citrix env                                |

## Related Documentation

Refer to the following documents for additional Catalyst 4500 series information:

- Catalyst 4500 Series Switch Documentation Home  
<http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html>
- Catalyst IOS-XE Release 3E Documentation Roadmaps  
<http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-3e/products-documentation-roadmaps-list.html>

## Hardware Documents

Installation guides and notes including specifications and relevant safety information are available at the following URLs:

- *Catalyst 4500 E-series Switches Installation Guide*  
<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/catalyst4500e/installation/guide/Eseries.html>
- For information about individual switching modules and supervisors, refer to the *Catalyst 4500 Series Module Installation Guide* at:  
[http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/configuration/notes/OL\\_25315.html](http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/configuration/notes/OL_25315.html)
- *Regulatory Compliance and Safety Information for the Catalyst 4500 Series Switches*  
[http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/regulatory/compliance/78\\_13233.html](http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/regulatory/compliance/78_13233.html)
- Installation notes for specific supervisor engines or for accessory hardware are available at:  
[http://www.cisco.com/en/US/products/hw/switches/ps4324/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html)

## Software Documentation

Software release notes, configuration guides, command references, and system message guides are available at the following URLs:

- Release Notes—Cisco IOS Release Notes for the Catalyst 4500-E Series Switches are available at:  
<http://www.cisco.com/c/en/us/support/switches/catalyst-4500-series-switches/products-release-notes-list.html>
- Guides—The Catalyst 4900M, Catalyst 4948E, Catalyst 4948E-F Series Switches, Catalyst 4500 Series Switches, the Catalyst 4500-X Series Switches, and the Catalyst 4500-E Series Switches, leverage the same software configuration guide, command reference guide, and system message guide:
  - Software Configuration Guides:  
[http://www.cisco.com/en/US/products/hw/switches/ps4324/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html)
  - Command Reference Guides:  
[http://www.cisco.com/en/US/products/hw/switches/ps4324/prod\\_command\\_reference\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_command_reference_list.html)
  - System Message Guides:  
[http://www.cisco.com/en/US/products/hw/switches/ps4324/products\\_system\\_message\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps4324/products_system_message_guides_list.html)

## Cisco IOS Documentation

Platform-independent Cisco IOS documentation is available at the following URLs:

- Cisco IOS configuration guides, Cisco IOS XE Release 3E

<http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-3e/products-installation-and-configuration-guides-list.html>

- Cisco IOS Master Command List. All Releases

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html>

You can also use the Command Lookup Tool at:

<http://tools.cisco.com/Support/CLILookup/cltSearchAction.do>

- You can also use the Error Message Decoder tool at:

<http://www.cisco.com/pegi-bin/Support/Errordecoder/index.cgi>

## Commands in Task Tables

Commands listed in task tables show only the relevant information for completing the task and not all available options for the command. For a complete description of a command, refer to the command in the *Catalyst 4500 Series Switch Cisco IOS Command Reference*.

## Notices

The following notices pertain to this software license.

### OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

#### **OpenSSL License:**

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:  
 “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

**Original SSLeay License:**

Copyright © 1995-1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). All rights reserved.

This package is an SSL implementation written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:  
 “This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com))”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

---

This document is to be used in conjunction with the documents listed in the “Notices” section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

© 2015-2019 Cisco Systems, Inc. All rights reserved.

