Release Notes for the Cisco Catalyst 4500E Series Switch, Cisco IOS XE 3.11.xE

First Published: 2019-03-27

Last Modified: 2024-03-29

Release Notes for the Catalyst 4500E Series Switch, Cisco IOS XE 3.11.xE

Introduction

This release note describes the features, modifications, and caveats for the Cisco IOS XE Release 3.11.xE, on the Cisco Catalyst 4500E Series Switches with Supervisor Engine 9-E, 8L-E, 8-E, 7L-E, and 7-E.

Note End-of-Life has been announced for Cisco Catalyst 4500 Supervisor Engine 7-E and Cisco Catalyst 4500 Supervisor Engine 7L-E.

Cisco IOS XE Release 3.11.xE is a feature rich new software feature release for Cisco IOS-XE based Catalyst Access Switching products.

Note Although Cisco Catalyst 4500E Series Switches and Cisco Catalyst 4500-X Series Switches have separate release notes, each leverages the same Software Configuration Guide and Command Reference Guide.

Cisco IOS Software Packaging

Cisco Catalyst 4500E Series Switches support these license levels or feature sets.

The following permanent right-to-use licenses or base licenses are available:

- Enterprise Services—image supports all Cisco Catalyst 4500E Series software features based on Cisco IOS Software, including enhanced routing.
- IP Base
- LAN Base

Starting with Cisco IOS XE Release 3.10.0E, the following add-on license options are available:

- DNA Essentials
- DNA Advantage

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

Cisco IOS XE Release Strategy

Cisco IOS XE Release 3.11.xE, 3.8.xE, 3.6.xE, 3.4.xSG, and 3.2.xSG are extended maintenance (EM) releases.

Cisco IOS XE Release 3.10.xE, 3.9.xE, 3.7.xE, 3.5.xE, and 3.3.0SG are standard maintenance releases (SM).

Cisco IOS XE Release 3.10.0E and later releases support Sup9-E.

Cisco IOS XE Release 3.8.1E and later releases support Sup8L-E.

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

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

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

Support

Support for Cisco IOS XE Release 3.11.xE follows the standard Cisco Systems® support policy, available at

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 4500-E Series Switch

Table 1: Supported Hardware on Cisco Catalyst 4500-E

Product Number (append with "=" for spares)	Product Description
WS-X45-Sup7-E	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E **Note** This engine is supported on E-series, R-E, and R+E chassis.
WS-X45-Sup7L-E	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E **Note** This engine is supported on E-series, R-E, and R+E chassis.
WS-X45-Sup8-E	Cisco Catalyst 4500 E-Series Supervisor Engine 8-E This engine is supported on E-series and R+E and R-E[1] chassis.

Product Number (append with "=" for spares)	Product Description
WS-X45-Sup8L-E	Cisco Catalyst 4500 E-Series Supervisor Engine 8L-E This engine is supported on E-series and R+E and R-E 1 chassis.
WS-X45-SUP9-E	Cisco Catalyst 4500 E-Series Supervisor Engine 9-E. This engine is supported on E-series and R+E chassis.
10 Gigabit Ethernet Switching Modules	
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
Gigabit Ethernet Switching Modules	
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-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-X4418-GB	18-port 1000BASE-X (GBIC) Gigabit Ethernet 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.

Product Number (append with "=" for spares)	Product Description
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 and7LE, but not on Supervisor Engines 8E and 8LE. This module is not supported in VSS mode.
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 and7L-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

Product Number (append with "=" for spares)	Product Description
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
Fast Ethernet Switching Modules	
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.
Ethernet/Fast Ethernet (10/100) Switching Modules	
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

Product Number (append with "=" for spares)	Product Description
WS-X4148-RJ21	48-port 10/100 4xRJ-21 (telco connector) switching module. Not supported in VSS mode.
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.
Other Modules	
MEM-X45-2GB-E	SD Card, 2G
USB-X45-4GB-E	USB Thumb Drive, 4G

[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.

Table 2: Supported Pluggable Transceiver Modules

Module Type	URL
Cisco 10-Gigabit Ethernet Transceiver Modules Compatibility Matrix	http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/10GE_Tx_Matrix.html
Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix	http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/GE_Tx_Matrix.html
Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix	http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/100MB_Tx_Matrix.html
Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix	http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/40GE_Tx_Matrix.html
Cisco Wavelength Division Multiplexing Transceivers Compatibility Matrix	http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6982.html

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

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

Supported E-Series Hardware on Cisco IOS XE Release 3.11.xE

A brief list of primary E-Series hardware supported by Cisco IOS XE Release 3.11.xE is shown in the following table:

Table 4: Supported E-Series Hardware

Product Number	Description
WS-C4503-E	Cisco Catalyst 4500-E Series 3-Slot Chassis • Fan tray • No Power Supply
WS-C4506-E	Cisco Catalyst 4500-E Series 6-Slot Chassis • Fan tray • No Power Supply

Product Number	Description
WS-C4507R-E	Cisco Catalyst 4500-E Series 7-Slot Chassis. **Note** The chassis does not support Supervisor Engine 9-E. The chassis requires hardware revision 2.0 or higher to support Supervisor Engines 8-E and 8L-E. • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 3 and/or 4; the backplane will enforce this restriction.
WS-C4507R+E	Cisco Catalyst 4500-E Series 7-Slot 48 GB-ready Chassis. • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 3 and/or 4; the backplane will enforce this restriction.
WS-C4510R-E	Cisco Catalyst 4500-E Series 10-Slot Chassis **Note** This chassis does not support Supervisor Engines 9-E, 8L-E, and 7L-E. • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 5 and/or 6; the backplane will enforce this restriction.

Product Number	Description
WS-C4510R+E	Cisco Catalyst 4500-E Series 10-Slot 48 GB-ready Chassis **Note** This chassis does not support Supervisor Engines 7L-E and 8L-E. • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 5 and/or 6; the backplane will enforce this restriction.

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

Th folloiwng table is a detailed list of features supported on Cisco Catalyst 4500 E-Series Supervisor Engines 9-E, 8L-E, 8-E, 7L-E, and 7-E running Cisco IOS XE Release 3.11.xE categorized by image type.

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

Table 5: LAN Base, IP Base, and Enterprise Services Image supported on Cisco Catalyst 4500 E-Series Supervisor Engines 9-E, 8L-E, 8-E, 7L-E, and 7-E

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

Feature	LAN Base	IP Base	Enterprise Services
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
Application Visibility and Control with Domain Name System-Authoritative Source (AVC with DNS-AS)	No	Yes	Yes
FNF for AVC with DNS-AS	No	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

Feature	LAN Base	IP Base	Enterprise Services
AutoQoS—VoIP	Yes	Yes	Yes
AutoRP Enhancement	No	Yes	Yes
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

Feature	LAN Base	IP Base	Enterprise Services
BGP Wildcard	No	No	Yes
Bidirectional PIM (IPv4 only)	Yes	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
Call Home	No	Yes	Yes
Campus Fabric	No	Yes (Sup 8-E, 9-E)	Yes (Sup 8-E, 9-E)
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

Feature	LAN Base	IP Base	Enterprise Services
Cisco-Port-QoS-MIB—Support for cportQosQueueEnqueuePkts and cportQosQueueDropPkts	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
Class-Based Marking	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
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—Configuration Agent, Event Agent, Image Agent, Interactive CLI, 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; 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

Feature	LAN Base	IP Base	Enterprise Services
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
DBL (Dynamic Buffer Limiting) - Selective DBL	Yes	Yes	Yes
Debounce Timer per Port	Yes	Yes	Yes
Default Passive Interface	No	Yes	Yes
Diffserv MIB	Yes	Yes	Yes
DHCP Client	Yes	Yes	Yes
DHCP Configurable DHCP Client	Yes	Yes	Yes
DHCP Gleaning	No	Yes	Yes
DHCP Option 82, Pass Through	Yes	Yes	Yes
DHCPv6 Ethernet Remote ID option	Yes	Yes	Yes
DHCPv6 Option 18	Yes	Yes	Yes
DHCPv6 Option 37 (Relay Options Remote-ID)	Yes	Yes	Yes
DHCPv6 Option 52 (CAPWAP Access Controller)	No	Yes	Yes
DHCPv6 Relay Agent notification for Prefix Delegation	Yes	Yes	Yes
DHCPv6 Relay - Reload persistent Interface ID option	Yes	Yes	Yes
DHCPv6 Repackaging	Yes	Yes	Yes
DHCP Server	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
DHCP Snooping	Yes	Yes	Yes
DSCP/CoS via LLDP	Yes	Yes	Yes
Duplication Location Reporting Issue	Yes	Yes	Yes
Dynamic Trunking Protocol (DTP)	Yes	Yes	Yes
Easy Virtual Network (EVN)	No	No	Yes
Easy VSS[2]	No	Yes (SUP 9-E, 8-E and 7E only)	Yes (SUP 9-E, 8L-E, 8-E, 7L-E, and 7E)
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
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

Feature	LAN Base	IP Base	Enterprise Services
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

Feature	LAN Base	IP Base	Enterprise Services
Flexible NetFlow —CTS Fields, Device Type, Ethertype, Full Flow Support, Ingress support, IPv4 and IPv6 Unicast Flows, Layer 2 Fields, Multiple User Defined Caches, Netflow Export over IPv4, NetFlowV5 Export protocol, NetFlow V9 Export Format, Power Reading, Username, VLAN ID support, Export to an IPv6 address, 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

Feature	LAN Base	IP Base	Enterprise Services
HTTP TACAC+ Accounting support	Yes	Yes	Yes
IEEE 802.1ab LLDP (Link Layer Discovery Protocol) 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[3]	Yes	Yes	Yes
IEEE 802.1w Spanning Tree Rapid Reconfiguration	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
IEEE 802.1x Auth Fail Open (Critical Ports) IEEE 802.1x Auth Fail VLAN IEEE 802.1x Flexible Authentication IEEE 802.1x Multiple Authentication IEEE 802.1x Open Authentication IEEE 802.1X with User Distribution IEEE 802.1x VLAN Assignment IEEE 802.1x VLAN User Group Distribution IEEE 802.1x Wake on LAN Support IEEE 802.1x Authenticator IEEE 802.1x Fallback support IEEE 802.1x Guest VLAN IEEE 802.1x Multi-Domain Authentication IEEE 802.1x Private Guest VLAN IEEE 802.1x Private VLAN Assignment	Yes	Yes	Yes
IEEE 802.1x RADIUS Accounting IEEE 802.1x RADIUS-Supplied Session Timeout	Yes	Yes	Yes
IEEE 802.1x with ACL Assignments IEEE 802.1x with Port Security	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
IEEE 802.3ad Link Aggregation (LACP) 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 IGMP Filtering IGMP Snooping IGMP Version 1 IGMP Version 2 IGMP Version 3 IGMP Version 3 - Explicit Tracking of Hosts, Groups, and Channels	Yes	Yes	Yes
IGMPv3 Host Stack 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

Feature	LAN Base	IP Base	Enterprise Services
IP Enhanced IGRP Route Authentication	No	No	Yes
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: Distribution of Statistics	No	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
IP SLAs — DNS Operation DNS Operation FTP Operation HTTP Operation ICMP Echo Operation ICMP Path Echo Operation Multi Operation Scheduler One Way Measurement Path Jitter Operation Random Scheduler Reaction Threshold Responder Scheduler Sub-millisecond Accuracy Improvements TCP Connect Operation UDP Based VoIP Operation UDP Echo Operation UDP Jitter Operation Video Operations VoIP Threshold Traps	Yes	Yes	Yes
IP Summary Address for RIPv2	Yes	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 OGACLs	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
IPv4 Policy-Based Routing IPv4 Policy-Based Routing with recursive next hop	Yes	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	Yes	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

Feature	LAN Base	IP Base	Enterprise Services
IPv6 First Hop Security (FHS) Phase 2: Binding table recovery Lightweight DHCPv6 Relay Agent (LDRA) IPv6 Snooping (Data Gleaning, per-limit Address Limit) Neighbor Discovery (ND) Multicast Suppress Source and Prefix Guard[4] FHS EtherChannel Support	Yes	Yes	Yes
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 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	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
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 PIM Embedded RP Support PIM Source-Specific Multicast (PIM-SSM) PIM Sparse Mode (PIM-SM)	Yes	Yes	Yes
IPv6 Multicast — Routable Address Hello Option	No	Yes	Yes
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 OGACLs	Yes	Yes	Yes
IPv6 OSPFv3 NSF/SSO	No	Yes[4]	Yes
IPv6 OSPFv3 Fast Convergence	Yes	Yes[4]	Yes
IPv6 PACL	Yes	Yes	Yes
IPv6 Policy-Based Routing	Yes	No	Yes

Feature	LAN Base	IP Base	Enterprise Services
IPv6 RA Guard (Host Mode)	Yes	Yes	Yes
IPv6 Router Advertisement Options for Domain Name System (DNS) Configuration	Yes	Yes	Yes
IPv6 Routing — EIGRP Support	No	No	Yes
IPv6 Routing — OSPF for IPv6 (OSPFv3)	Yes	Yes[5]	Yes
IPv6 Routing — RIP for IPv6 (RIPng)	Yes	Yes	Yes
IPv6 Routing — Route Redistribution	No	Yes	Yes
IPv6 Routing — Static Routing	Yes	Yes	Yes
Pv6 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 DNS Lookups over an IPv6 Transport Extended Access Control Lists Standard Access Control Lists	Yes	Yes	Yes
IPv6 Stateless Auto-configuration	Yes	Yes	Yes
IPv6 Static Routing: Support for Tracking Objects	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
IPv6 Support for SGT/SGACL	Yes	Yes	Yes
IPv6 Switching: CEF Support CEFv6 Switched Automatic IPv4-compatible Tunnels (in software) CEFv6 Switched ISATAP Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: Automatic 6 to 4 Tunnels (in software) Automatic IPv4-compatible Tunnels (in software) IPv6 over IPv4 GRE Tunnels (in software) ISATAP Tunnel Support (in software) 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

Feature	LAN Base	IP Base	Enterprise Services
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
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
Master Key Agreement (MKA) MACsec with EAP-TLS • Switch-to Switch Connections with Pre-Shared Keys • Port Channels	Yes	Yes	Yes
Medianet — AutoQoS SRND4 Macro	No	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
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

Feature	LAN Base	IP Base	Enterprise Services
Multigigabit Ethernet Interface — Downshift Speed	Yes	Yes	Yes
NAC — L2 IEEE 802.1x	Yes	Yes	Yes
NAC — L2 IP	Yes	Yes	Yes
Named VLAN	Yes	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
NAC — L2 IEEE 802.1x	Yes	Yes	Yes
Network Time Protocol (NTP) NTP primary (formerly known as NTP master)	Yes	Yes	Yes
Next Hop Resolution Protocol (NHRP)	No	No	Yes
NMSP Enhancements • GPS support for location • GPS support for location Location at switch level • Local timezone change • Name value pair • Priority settings for MIBs	No	Yes	Yes
No Service Password Recovery	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
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 Tracking: IPv6 Route Tracking	No	Yes	Yes
Onboard Failure Logging (OBFL)	Yes	Yes	Yes
Open Plug-N-Play Agent	Yes	Yes	Yes
OSPF OSPF v3 Authentication OSPF Flooding Reduction	Yes	Yes[4]	Yes
OSPF for Routed Access[6]	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
OSPF Incremental Shortest Path First (i-SPF) Support OSPF Link State Database Overload Protection OSPF Not-So-Stubby Areas (NSSA) OSPF Packet Pacing OSPF Shortest Paths First Throttling OSPF Stub Router Advertisement OSPF Support for Fast Hellos OSPF Support for Link State Advertisement (LSA) Throttling OSPF Update Packet-Pacing Configurable Timers	Yes	Yes[4]	Yes
OSPF Support for Multi-VRF on CE Routers	No	Yes[4]	Yes
PBR Support for Multiple Tracking Options PBR with Object Tracking	Yes	Yes	Yes
Per Intf IGMP State Limit Per Intf MrouteState Limit Per Port Per VLAN Policing Per-User ACL Support for 802.1X/MAB/Webauth users Per-VLAN Learning	Yes	Yes	Yes
Permanent Right-to-Use (PRTU) license	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
PIM Dense Mode State Refresh PIM Multicast Scalability PIM Version 1 PIM Version 2	Yes	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)s
Port Security on Etherchannel Trunk Port 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 Private VLAN Trunk Ports Private VLANs	Yes	Yes	Yes
Programmability	Yes	Yes	Yes
Propagation of Location Info over CDP	Yes	Yes	Yes
PVLAN over EtherChannel 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	No	No	No

Feature	LAN Base	IP Base	Enterprise Services
RADIUS RADIUS Attribute 44 (Accounting Session ID) in Access Requests RADIUS Change of Authorization Rapid PVST+ Dispute Mechanism Rapid-Per-VLAN-Spanning Tree Plus (Rapid-PVST+) Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)	Yes	Yes	Yes
Reduced MAC Address Usage	Yes	Yes	Yes
Redundancy Facility Protoco	Yes	Yes	Yes
Remote SPAN (RSPAN)	Yes	Yes	Yes
REP (Resilient Ethernet Protocol) REP — No Edge Neighbor Enhancement	Yes	Yes	Yes
RIP v1	Yes	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 Secure Copy (SCP)	Yes	Yes	Yes
Secure Shell SSH Version 2 Client Support Secure Shell SSH Version 2 Server Support	Yes	Yes	Yes
Security Group ACL at Interface Level	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
Single Rate 3-Color Marker for Traffic Policing	Yes	Yes	Yes
Smart Port	Yes	Yes	Yes
SNMP (Simple Network Management Protocol) SNMP Inform Request SNMP Manager SNMPv2C SNMPv3 — 3DES and AES Encryption Support SNMPv3 (SNMP Version 3)	Yes	Yes	Yes
Source Specific Multicast (SSM) Source Specific Multicast (SSM) - IGMPv3,IGMP v3lite, and URD 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 SPAN — Packet Type and Address Type Filtering	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
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 Sticky Port Security on Voice VLAN	Yes	Yes	Yes
Storm Control Storm Control — Per-Port Multicast Suppression	Yes	Yes	Yes
STP Syslog Messages	Yes	Yes	Yes
Stub IP Multicast Routing	Yes	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
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) Switch Port Analyzer (SPAN) - CPU Source	Yes	Yes	Yes
Syslog over IPV6	Yes	Yes	Yes
System Logging - EAL4 Certification Enhancements	Yes	Yes	Yes
TACACS SENDAUTH function TACACS Single Connection TACACS+ TACACS+ and Radius for IPv6-	Yes	Yes	Yes
TCAM4 — Dynamic Multi-Protocol TCAM4 — Service-Aware Resource Allocation	Yes	Yes	Yes
Time Domain Reflectometry (TDR)[7]	Yes	Yes	Yes
Time-Based Access Lists 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

Feature	LAN Base	IP Base	Enterprise Services
Uni-Directional Link Routing (UDLR)	No	Yes	Yes
Unicast Mac Filtering	Yes	Yes	Yes
Unicast Reverse Path Forwarding (uRPF)	No	Yes	Yes
Unidirectional Ethernet UniDirectional Link Detection (UDLD)	Yes	Yes	Yes
UDP Forwarding Support for IP Redundancy Virtual Router Group	Yes	Yes	Yes
Virtual Router Redundancy Protocol (VRRP) for IPv4	No	Yes	Yes
Virtual Switching System (VSS)	No	Yes (Sup 7-E and Sup 8-E only)	Yes (Sup 7-E, Sup 7L-E, Sup 8-E, and Sup 8L-E)
VSS — Layer 2 Protocol Tunneling, VLAN Translation, and Q-in-Q VSS — REP, Flexlinks, UDLD, Fast UDLD	No	Yes	Yes
Virtual Trunking Protocol (VTP) — Pruning	Yes	Yes	Yes
VLAN Access Control List (VACL) VLAN MAC Address Filtering	Yes	Yes	Yes
VLAN Mapping (VLAN Translation) VLAN Switching and Selective QinQ on the Same Port	No	Yes	Yes

Feature	LAN Base	IP Base	Enterprise Services
VRF-aware Copy Commands VRF-aware SGT (Subnet-to-SGT mapping and VLAN-to-SGT mapping)	No	Yes	Yes
VRF-aware PBR VRF-aware TACACS+ VRF-aware WCCP for IPv4 traffic VRF-aware WCCP for IPv6 traffic	No	No	Yes
VRF-lite for IPv6 on OSPF/ BGP/ EIGR	No	No	Yes
VRRPv3 — Object Tracking Integration VRRPv3 Protocol Support	No	Yes	Yes
VTP (Virtual Trunking Protocol) Version 2 VTP Version 3	Yes	Yes	Yes
WCCP Version 2 WCCP Version 2 on VSS WCCP Version 2 for IPv6	No	Yes	Yes
Web Authentication Proxy Web Authentication Redirection to Original URL Webauth Enhancements	Yes	Yes	Yes
Wired Guest Access[8]	No	Yes	Yes
Wireshark-based Ethernet Analyzer	No	Yes	Yes
XML-PI	Yes	Yes	Yes

[2.] Supervisor Engine 7-E, and Supervisor Engine 8-E, Supervisor Engine 8L-E; IP Base. Supervisor Engine 7L-Ent Services

[3] IEEE 802.1t—An IEEE amendment to IEEE 802.1D that includes extended system ID, long path cost, and PortFast.
[4] 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
[5] IP Base supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 200 dynamically learned routes.
[6] OSPF for Routed Access supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 1000 dynamically learned routes.
[7] TDR is not supported on 46xx linecards.
[8] 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
Cisco Catalyst 4500E Series Switches with Supervisor Engine 9-E	IOS XE 3.11.0E	2.0.2	ofa-2.0.2-r2-cat4500es8-SPA-k9.ova	cat4500es8-universalk9.SPA.03.11.00.E.152-7.E.bin
Cisco Catalyst 4500E Series Switches with Supervisor Engine 8L-E, 8-E	IOS XE 3.11.0E	2.0.2	ofa-2.0.2-r2-cat4500es8-SPA-k9.ova	
Cisco Catalyst 4500E Series Switches with Supervisor Engine 7L-E, 7-E	IOS XE 3.11.0E	2.0.2	ofa-2.0.2-r2-cat4500es8-SPA-k9.ova	cat4500e-universalk9.SPA.03.11.00.E.152-7.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

The following table lists the Cisco IOS XE Release 3.11.xE Product Numbers and Images for the Catalyst 4500-E Series Switch

Product Number	Description	Image
S45EULPE-S8-38E	CAT4500e SUP8-E /SUP8L-E Universal NoMACSEC Image	cat4500es8-universalk9npe
S45EUK9-S8-38E	CAT4500e SUP8-E/SUP8L-E 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-universalk9np
S45EU-S8-38E	CAT4500e SUP8L-E Universal Image	cat4500es8-universal
S45EU-S7-38E	CAT4500e SUP7-E/SUP7L-E Universal Image	cat4500e-universal

New and Changed Information

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

New Features in Cisco IOS XE Release 3.11.11E

New Software Features

None.

New Features in Cisco IOS XE Release 3.11.10E

New Software Features

None.

New Features in Cisco IOS XE Release 3.11.9E

New Software Features

None.

New Features in Cisco IOS XE Release 3.11.8E

New Software Features

Feature	Description
Secure Data Wipe	Introduces support for performing factory reset by using the keyword **all secure** in the **factory-reset** command. This option performs data sanitisation and securely resets the device.

New Features in Cisco IOS XE Release 3.11.7E

None.

New Features in Cisco IOS XE Release 3.11.6E

None.

New Features in Cisco IOS XE Release 3.11.5E

None.

New Features in Cisco IOS XE Release 3.11.4E

None.

New Features in Cisco IOS XE Release 3.11.3aE

New Software Features

Feature	Description
Support for Type 6 AES Encryption password	Beginning with this release, you can specify a Type 6 encrypted key for a TACACS Server. The new command is **tacacs server key 6** *key-name*. **Note** Before downgrading from Cisco IOS XE Release 3.11.3aE to an earlier release, ensure that Type 6 encryption is removed from the TACACS Server. (Type 6 encryption is not supported in releases earlier than Cisco IOS XE Release 3.11.3aE.)

New Features in Cisco IOS XE Release 3.11.2E

None.

New Features in Cisco IOS XE Release 3.11.1E

New Software Features in IOS XE 3.11.1E

Feature Name	Description
Support for IPv6 DACL	This release supports downloadable ACLs for devices with IPv6 address. You can download the authorization policies from the Identity Services Engine (ISE) server.

New Features in Cisco IOS XE Release 3.11.0E

New Software Features

Feature Name	Description
SSH File Transfer Protocol Support	Secure Shell (SSH) includes support for SSH File Transfer Protocol (SFTP), a new standard file transfer protocol introduced in SSHv2. This feature provides a secure and authenticated method for copying device configuration or device image files.
PVLAN Support with Multicast	Multicast traffic is now supported with PVLAN. Multicast traffic is routed or bridged across private-VLAN boundaries and within a single community VLAN.

Cisco IOS XE to Cisco IOS

Each version of Cisco IOS XE has an associated Cisco IOS version:

Table 7: 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
03.9.0E	15.2(5)E	10.5.100.0	15.3(3)JND
03.10.0E	15.2(6)E	-	-
03.10.1E	15.2(6)E1	-	-
03.10.2E	15.2(6)E2	-	-
03.11.0E	15.2(7)E	-	-
03.11.1E	15.2(7)E1	-	-
03.11.1aE	15.2(7)E1a	-	-
03.11.2E	15.2(7)E2	-	-
03.11.3aE	15.2(7)E3	-	-
03.11.4E	15.2(7)E4	-	-
03.11.5E	15.2(7)E5	-	-
03.11.6E	15.2(7)E6	-	-

Upgrading the System Software

For details about the required ROMMON version and to know how to upgrade the ROMMON, refer to:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/release/note/OL_30306-01.html

Follow these guidelines:

- Before upgrading to Cisco IOS XE Release 3.11.3aE, ensure the following:
    - Remove the **tacacs-server** command configuration using its **no** form.
    - Configure the TACACS Server using the new **tacacs server** command.
    - If the TACACS group server is configured using the **server-private** CLI, unconfigure the private server and configure a public server using the **server name** *server-name* command.
- If you are upgrading to Cisco IOS XE Release 3.9.xE and using Supervisor Engine 8L-E, you must upgrade to ROMMON 15.1(1r)SG6 before upgrading the IOS-XE image to 3.9.0E or newer versions.
- If you are upgrading to Cisco IOS XE Release 3.9.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 3.9.xE and using Supervisor Engine 7-E or 7L-E, we recommend that you use ROMMON version 15.0(1r)SG10 or a higher version (if available).
- If you are upgrading to Cisco IOS XE Release 3.9.xE and using Supervisor Engine 8-E, we recommend that you use ROMMON version 15.1(1r) SG5 or later version (if available).
- 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).
- Do not perform a ROMMON upgrade and a system software (IOS) upgrade together, if it involves an RPR failover. After such an upgrade, one of the Supervisor's interface configurations are lost (CSCvu66041).

  We recommend that you use an ISSU compatible IOS image for an IOS upgrade that is done along with a ROMMON upgrade. To display the ISSU compatibility matrix data between two software images on a given system, use the **show issu comp-matrix stored** command.

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>
```

Limitations and Restrictions

- In Cisco IOS XE Release 3.11.3aE and later releases, SSH is enabled by default to connect to networks, and Telnet is disabled by default.
- TACACS legacy command: Do not configure the legacy **tacacs-server host** command; this command is deprecated. If the software version running on your device is Cisco IOS XE 3.11.3aE or a later release, using the legacy command can cause authentication failures. Use the **tacacs server** command in global configuration mode.
- RADIUS Server legacy command: In Cisco IOS XE Release 3.8.7E, the legacy **radius-server host** command is deprecated. Use the **radius server host** command if the software running on your device is Cisco IOS XE Release 3.8.7E or later.
- During an ISSU downgrade from IOS XE 3.11.1E to IOS XE 03.08.09 version, the standby is loaded with the main image. This is due to failure of configuration synchronization on device tracking and ACL.

  Workaround:

  - Before an ISSU downgrade, revert the device-tracking CLI to legacy CLI:

    ```
    Device# configure terminal
    Device(config)# device-tracking upgrade-cli revert
    ```

  - Before an ISSU downgrade, delete the numbered ACLs from the primary and reapply them after the downgrade process.

- ISSU or Fast Software Upgrade (FSU) limitations:
  - When upgrading to Cisco IOS XE Release 3.11.0E, or Cisco IOS XE Release 3.8.7E, or Cisco IOS XE Release 3.10.2E with ISSU or FSU, if you are using a multi-Gigabit Ethernet linecard, reload the linecard after the upgrade to avoid interface issues.
  - When downgrading from Cisco IOS XE Release 3.11.0E and later, or Cisco IOS XE Release 3.8.7E and later, or Cisco IOS XE Release 3.10.2E and later with ISSU or FSU, if you are using a multi-Gigabit Ethernet linecard, reload the linecard after upgrade to avoid interface issues.

- Starting with Cisco IOS XE Release 3.9.0E, Secure Shell (SSH) Version 1 is deprecated. Use SSH Version 2 instead.

- 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
    - blank.gif 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, 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 an 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 slvecrashinfo-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 x 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.
- An 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" />
  ```

  produces 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 policymap <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 causes 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

- 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).

Caveats

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

Cisco Bug Search Tool

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

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

Open Caveats in Cisco IOS XE Release 3.11.11E

None.

Resolved Caveats in Cisco IOS XE Release 3.11.11E

Caveat ID Number	Description
CSCvv54811	17.4:ASR1K:RP crashed while runnint ISAKMP codenomicon suite

Caveat ID Number	Description
CSCwh66334	Cisco IOS and IOS XE Software IKEv1 Fragmentation Denial of Service Vulnerabilities
CSCwi59625	Cisco IOS and IOS XE Software Web UI Cross-Site Request Forgery Vulnerability
CSCwj05481	Cisco IOS and IOS XE Software Resource Reservation Protocol Denial of Service Vulnerability

Open Caveats in Cisco IOS XE Release 3.11.10E

None.

Resolved Caveats in Cisco IOS XE Release 3.11.10E

Caveat ID Number	Description
CSCwf54007	Cisco IOS and IOS XE Software IS-IS Denial of Service Vulnerability
CSCwe55871	Cisco IOS and Cisco IOS XE Software Command Authorization Bypass Vulnerability

Open Caveats in Cisco IOS XE Release 3.11.9E

None.

Resolved Caveats in Cisco IOS XE Release 3.11.9E

Caveat ID Number	Description
CSCwh38827	C4500X: Traffic impacted via tunnel when upgrading to 3.11.x version

Open Caveats in Cisco IOS XE Release 3.11.8E

None.

Resolved Caveats in Cisco IOS XE Release 3.11.8E

Caveat ID Number	Description
CSCwa34310	Cisco IOS and IOS XE Software IPv6 DHCP (DHCPv6) Client Denial of Service Vulnerability

Open Caveats in Cisco IOS XE Release 3.11.7E

None.

Resolved Caveats in Cisco IOS XE Release 3.11.7E

Caveat ID Number	Description
CSCvp12187	Standby switch crash because of memory leak due to Switch Integrated security feature.
CSCwc66348	RBACL not downloaded on previously shutdown port.
CSCvw60355	DHCPv6: Memory allocation of DHCPv6 relay option results in crash.
CSCvx63027	Cisco IOS and IOS XE Software SSH Denial of Service Vulnerability.
CSCwa96810	Cisco IOS and IOS XE Software Common Industrial Protocol Request Denial of Service Vulnerability.

Open Caveats in Cisco IOS XE Release 3.11.6E

None.

Resolved Caveats in Cisco IOS XE Release 3.11.6E

Caveat ID Number	Description
CSCwa22165	Incorrect access list logging during SSH session.
CSCvz22651	Memory leak due to csmControllerStatistics on Cisco Catalyst 4000 Series Switches.
CSCvz09717	Cisco Catalyst 4500 -PC connected to a standby VSS switch is not getting the IP address post user authentication.
CSCvz42464	Cisco QSFP-40G-LR4 incompatible with WS-X45-SUP9-E.

Open Caveats in Cisco IOS XE Release 3.11.5E

None.

Resolved Caveats in Cisco IOS XE Release 3.11.5E

Caveat ID Number	Description
CSCvg65857	link debounce CLI disappears when shut member port in LAG.
CSCvw75254	C4500X TX-Queue zeroed out on VSL.

Caveat ID Number	Description
CSCvx36584	Intermittent working of PBR on 4500 with GRE tunnel as next hop.
CSCvx43251	ZTP fails to configure c4500e with dual-SUP when in-band port are used to reach the DHCP/TFTP server.
CSCvx47020	Segmentation fault in CMI IOSd task when running multicast.
CSCvx56995	once posture ACL is un-installed (post CoA), open-dir-acl wont get applied.
CSCvx94899	EAP-MSCHAPv2 isn't compliant with response size.
CSCvy12052	Catalyst Switch crashes @ sisf_sw_policy_detach_target.
CSCvy17077	RxErrorBytes on certain superports following an LC reload.
CSCvy67787	C4510RE Etherchannel ports on dual Supervisors go to suspended mode after switchover.
CSCvx76066	Switch crashes due to "HTTP Core".
CSCvx66699	Cisco IOS and IOS XE Software TrustSec CLI Parser Denial of Service Vulnerability.

Open Caveats in Cisco IOS XE Release 3.11.4E

Caveat ID Number	Description
CSCvx36584	Intermittent working of PBR on 4500 with GRE tunnel as next hop
CSCvx47020	Segmentation fault in CMI IOSd task when running multicast
CSCvx56995	once posture ACL is un-installed (post CoA), open-dir-acl wont get applied
CSCvx66968	C4500 relay agent drops DHCP offer when certain relay agent settings configured

Resolved Caveats in Cisco IOS XE Release 3.11.4E

Caveat ID Number	Description
CSCvu24091	GLC-T /TE not linking up sometimes on BOOTUP
CSCvv25129	3.11.2 - Cat4500X may crash unexpected when trying to program IPv6 to SGT mapping
CSCvv54294	IPDT probe uses physical interface MAC as source instead of SVI MAC in 3.11.x release

Caveat ID Number	Description
CSCvv56133	4500x in VSS may see VSL links in an up/down state after reboot when using Twin-ax cables
CSCvv86851	TACACS not working if TACACS group server has "server-private <ip> key <passw>" in 15.2(7)E3/3.11.3E
CSCvv93417	Stack Member Switch fails wired dot1x; MasterSwitch passes dot1x using the same configs
CSCvw45946	Cat4K multicast stop after REP node power cycle
CSCvw48485	K5L2 crash while fetching RET entry due to NULL entry.
CSCvx09751	Tracebacks seen after ISSU upgrade from 3.8.8 to 3.11.2E on 4500

Open Caveats in Cisco IOS XE Release 3.11.3aE

Caveat ID Number	Description
CSCvu24091	GLC-T /TE not linking up sometimes on BOOTUP
CSCvv79624	Interface does not come up when monitor session is removed

Resolved Caveats in Cisco IOS XE Release 3.11.3aE

Caveat ID Number	Description
CSCvv76539	1G CTS enabled links from Cat4K experience instability
CSCvs06645	%C4K_L2MAN-6-INVALIDSOURCEADDRESSPACKET: packets are forwarded to clients
CSCvs77826	Not able to scale beyond about 8K SGACLs on 4500, Traceback thrown for installation failure
CSCvt06123	C4500 Standby VSS Switch Crashing at XDR receive process
CSCvt09648	SGT propagation fails after sup failover
CSCvt12683	HTTP redirect doesn't work on 152-7.E1
CSCvt23492	c4500x VSS standby switch rapid memory exhaustion in IOSd due to process "MFIB_Cable"
CSCvt32280	GLC-TE on Cat4500X VSS sometimes may not link up after reload
CSCvu07615	Switches downstream of a Cat4k using 1g ports may see giants in the form of 1526B frames
CSCvu68040	C4500 No STP PVID inconsistent state when there is native vlan mismatch

Caveat ID Number	Description
CSCvu10399	Cisco IOS and IOS XE Software Information Disclosure Vulnerability
CSCvv00134	VTY telnet disable, enable ssh based on platform request

Open Caveats in Cisco IOS XE Release 3.11.2E

Caveat ID Number	Description
CSCvt23492	c4500x VSS standby switch rapid memory exhaustion in IOSd due to process "MFIB_Cable"
CSCvt28484	Cat4500X VSS may crash unexpected when program ACL's to TCAM
CSCvt32280	GLC-TE on Cat4500X VSS sometimes may not link up after reload

Resolved Caveats in Cisco IOS XE 3.11.2E

Caveat ID Number	Description
CSCvr87400	4500X : GLC-TE sometimes may not link up after reload
CSCvs58656	"vlan internal allocation policy" not displayed in show running-config all
CSCvs62898	Sup7L-E crash with "show platform hardware qos interface cpu tx-queue [dbl | scheduling]" command
CSCvs63040	DACL sent by the server that is not processed correctly by the switches 4500
CSCvs83434	DHCPv6 does not work due to LDRA

Resolved Caveats in Cisco IOS XE 3.11.1aE

Caveat ID Number	Description
CSCvi48253	Self-signed certificates expire on 00:00 1 Jan 2020 UTC, can't be created after that time

Open Caveats in Cisco IOS XE Release 3.11.2E

Caveat ID Number	Description
CSCvt23492	c4500x VSS standby switch rapid memory exhaustion in IOSd due to process "MFIB_Cable"
CSCvt28484	Cat4500X VSS may crash unexpected when program ACL's to TCAM
CSCvt32280	GLC-TE on Cat4500X VSS sometimes may not link up after reload

Resolved Caveats in Cisco IOS XE 3.11.1E

Caveat ID Number	Description
CSCut66603	Device stuck on 4500X VSS during Rommon version upgrade
CSCvi66577	Crash due null pointer after CISCO SFP failed the Gbic Integrity Check
CSCvi66866	Crash while polling of dot1dStaticEntry
CSCvk11391	Upgrade to 3.8.6 continuously reloads STANDBY supervisor in VSS
CSCvk57096	GLC-T Not Functioning in Ports 1, 5, 9, 13 on 4500X-16 in VSS standby
CSCvk74432	AFTER ADDING NEW VLAN IN REP SEGMENT THERE IS A LAYER 2 LOOP
CSCvm90630	4500 forwards traffic on BKN interface
CSCvn71215	Missing PBr config cuases crash on L3 rewrite
CSCvo07490	VSS switchover results in REP failure warnings
CSCvo08913	Can't ISSU from 3.8.6E to 3.10.2E due to an inconsistency between the Active and Standby
CSCvo09436	Cat4510 SUP8E - Active crashing while DFE training on Standby SUP
CSCvo24813	WS-C4510R+E / Dual WS-X45-SUP8-E / Crash when configuring flow exporter
CSCvo35887	CAT 4K Crashes Due to Watchdog Timeout When Opening Console TTY Session
CSCvo86432	Crash due to invalid entry in FIB Adjacency Table.
CSCvp11516	4500X with ACL config will crash when copying configuration
CSCvp24671	H/W mac address table learn wrong mac on C4500X VSS with active Flexlink shut/no shut
CSCvp33074	Cat4500 crashes due to multicast
CSCvp34354	4500X with GLC-TE sometimes may not link up after reload on 3.11.0E
CSCvp76408	Unable to generate RSA keys as long as a 46xx module ins installed in the chassis with SUP9
CSCvq30648	C4500 03.11.00.E (15.2(7)E) SNMP crash due to mediatrace config
CSCvq35190	DACL abnormal remove due to SISF.
CSCvq39976	SNMP Mac Move notification trap displays same interface ID for FromPortId and ToPortId
CSCvq90033	Multi-gig ports having connectivity issues on 4507/4510 switches on 3.11 code
CSCvq95472	Commands returning invalid PRC

Caveat ID Number	Description
CSCvr23923	Crash is observed after OIR or module reset of Mortis-CR PPLT linecards
CSCvr55005	Incorrect CTS tag sticks to flow, even when that tag is no more seen with flow

Open Caveats in Cisco IOS XE Release 3.11.0E

Caveat ID Number	Description
CSCvi66866	Crash while polling of dot1dStaticEntry
CSCvo83116	QuadSup VSS : Standby goes to disabled mode after 2nd switchover

Resolved Caveats in Cisco IOS XE 3.11.0E

Caveat ID Number	Description
CSCvm90630	4500 forwards traffic on BKN interface
CSCvm96180	Cat4500 switch reboots unexpectedly after certain Netflow configuration is pushed via SSH
CSCvn71215	Missing PBR config causes crash on L3 rewrite
CSCvn71260	Catalyst 4500 - CTS policy is not deleted in Hardware eventhough it is actually deleted.
CSCvo07490	VSS switchover results in REP failure warnings
CSCvo09436	Cat4510 SUP8E - Active crashing while DFE training on Standby SUP

Related Documentation

Refer to the Cisco Catalyst 4500E Series Switches Documentation Home for information:

https://www.cisco.com/c/en/us/support/switches/catalyst-4500-series-switches/tsd-products-support-series-home.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

- 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

- 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

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 4500-X Series Switches, and the Catalyst 4500-E Series Switches, leverage the same software configuration guide and command reference guide:

  – Software Configuration Guides:

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

  https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-10-0E/wireless/b_sda/fabric-enabled-wireless.html

  – Command Reference Guides: http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_command_reference_list.html

Cisco IOS Documentation

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

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

Communications, Services, and Additional Information

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