



Release Notes for the Catalyst 4500E Series Switch, Cisco IOS XE Release 3.4.xSG

Current release
IOS XE 3.4.8SG—Nov 11, 2016

Prior release
IOS XE 3.4.7 SG, IOS XE 3.4.6SG, IOS XE 3.4.5SG, IOS XE 3.4.4SG, IOS XE 3.4.3SG, XE 3.4.2SG, XE 3.4.1, XE 3.4.0SG

This release note describes the features, modifications, and caveats for the Cisco IOS XE 3.4.xSG software on the Catalyst 4500E series switch with Supervisor Engine 7-E and 7L-E.

Cisco IOS XE Software Release 3.4.2SG introduces the Permanent Right-to-Use (PRTU) license feature.

Cisco IOS XE Software Release 3.4.0SG delivers new software and hardware innovations in campus access and aggregation deployments that span across many technologies including Security, Video, High Availability, Network Virtualization, IP Multicast and Lower TCO as following:

High Availability

- Virtual Switching System (VSS)
 - Layer 2 Multichassis EtherChannel (MEC)
 - Enhanced Port Aggregation Protocol (ePAgP) split brain detection method
 - Cross-chassis Nonstop Forwarding with Stateful Switchover (NSF/SSO)
 - Cross-chassis in-service software upgrade (ISSU)
 - Support for Power over Ethernet (PoE) line card
 - Support for virtual switch link (VSL) on 1 Gigabit and 10 Gigabit links
 - All four ports on quad supervisor scenario may be used for uplink
- ISSU—IPv4 Multicast
- ISSU—IPv6 Multicast
- NSF/SSO—IPv4 Multicast
- NSF/SSO—IPv6 Multicast

Security

- IPv6 First Hop Security



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

© 1999-2012 Cisco Systems, Inc. All rights reserved.

- DHCPv6 Guard
- Lightweight DHCPv6 Relay Agent (LDRA)
- IPv6 Destination Guard
- IPv6 Snooping
- IPv6 Neighbor Discovery Multicast Suppression
- IPv6 Router Advertisement (RA) Guard
- Other
 - Reverse SSH Enhancements
 - Secure Shell SSH Version 2 Client Support
 - Secure Shell SSH Version 2 Server Support
 - SSH Keyboard Interactive Authentication
 - SSHv2 Enhancements
 - SSHv2 Enhancements for RSA Keys

Lower Total Cost of Ownership and Ease of Use

- Smart Install (Director Support)

Routing and Multicast Enhancements

- BGP Consistency Checker
- IPv6 BSR Scoped Zone support
- OSPFv3 Address Families
- OSPFv3 Time To Live Security
- Policy Based Routing: Recursive Next Hop

IPv6 Access Control

- IPv6 VACL (Vlan Access Control List)
- SPAN ACL Filtering for IPv6

Other

- FTP IPv6 Support
- IPSLA 4.0 - IPv6 phase 2
- IPSLA Multicast Support
- NTPv4 Orphan Mode support, Range for trusted key configuration
- TFTP IPv6 Support
- WSMA and XMLPI enhancement

Support for Cisco IOS XE Release 3.4.0SG follows the standard Cisco Systems® support policy, available at

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*.

Contents

This publication consists of these sections:

- [Cisco IOS Software Packaging, page 3](#)
- [Cisco XE Release Strategy, page 4](#)
- [System Requirements, page 5](#)
- [New and Changed Information, page 33](#)
- [Cisco IOS XE to Cisco IOS Version Number Mapping, page 35](#)
- [Upgrading the System Software, page 35](#)
- [Limitations and Restrictions, page 35](#)
- [Caveats, page 40](#)
- [Related Documentation, page 65](#)
- [Notices, page 67](#)

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), Internetwork Packet Exchange (IPX), AppleTalk, Virtual Routing Forwarding (VRF-lite), and policy-based routing (PBR).

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. The IP upgrade image is available if at a later date you require some of those features

Starting with Cisco IOS Release (3.3.0SG or 15.1(1)SG), support for IP SLAs and NSF have been extended from Enterprise Services to IP Base.

Topics include:

- [Feature Support by Image Type, page 12](#)
- [MIB Support, page 31](#)
- [Features Not Supported on the Cisco Catalyst 4500E Series Switch, page 31](#)
- [Orderable Product Numbers, page 32](#)

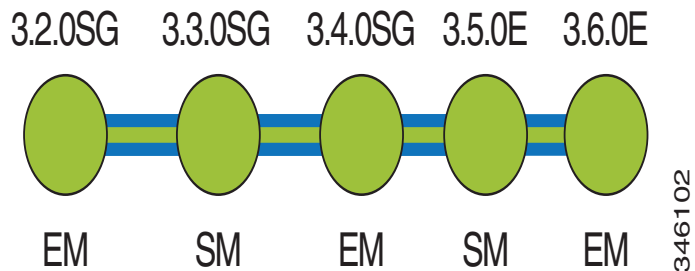
Cisco XE Release Strategy

Customers with Catalyst 4500 Series Switches who need the latest hardware and software features should migrate to Cisco IOS Release XE 3.4.0SG.

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, Sup7L-E and 4500X.

Figure 1 displays the two active trains: 3.2.xSG and 3.4.xSG.

Figure 1 Software Release Strategy for the Catalyst 4500E Series Switch



Support

Support for Cisco IOS Software Release XE 3.4.0SG 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 4500E Series Switch](#), page 5
- [Supported E Series Hardware on Cisco IOS XE Release 3.4.0SG](#), page 10
- [Feature Support by Image Type](#), page 12
- [MIB Support](#), page 31
- [Features Not Supported on the Cisco Catalyst 4500E Series Switch](#), page 31
- [Orderable Product Numbers](#), page 32

Supported Hardware on the Catalyst 4500E Series Switch

For information on the minimum supported release for each pluggable module please refer to:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Table 1 lists the hardware supported on the Catalyst 4500E Series Switch.



Note

Linecards with WS-X45xx and below are not supported in VSS.

Table 1 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-E

Product Number (append with “=” for spares)	Product Description
Supervisor Engines	
WS-X45-Sup7-E	Catalyst 4500E-series switch Supervisor Engine 7-E Note This engine is supported on E-series, R-E, and R+E chassis.
WS-X45-Sup7L-E	Catalyst 4500E-series switch Supervisor Engine 7L-E Note This engine is supported on E-series, R-E, and R+E chassis.
10 Gigabit Ethernet Switching Modules	
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
WS-X4306-GB	6-port 1000BASE-X (GBIC) Gigabit Ethernet switching module
WS-X4418-GB	18-port 1000BASE-X (GBIC) Gigabit Ethernet server switching module
WS-X4412-2GB-T	12-port 1000BASE-T Gigabit Ethernet and 2-GBIC ports switching module
WS-X4424-GB-RJ45	24-port 10/100/1000BASE-T Gigabit Ethernet RJ-45 switching module
WS-X4448-GB-LX	48-port 1000BASE-LX (small form-factor pluggable) Gigabit Ethernet fiber optic interface switching module

Table 1 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-E

Product Number (append with “=” for spares)	Product Description
WS-X4448-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet switching module
WS-X4448-GB-SFP	48-port 1000BASE-X (small form-factor pluggable) module
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
WS-X4524-GB-RJ45V	24-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af
WS-X4548-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet module
WS-X4548-GB-RJ45V	48-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af
WS-X4548-RJ45V+	48-port 10/100/1000 Premium PoE line card
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) Note WS-X4640-CSFP-E is not supported in a 10-slot chassis.
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
Fast Ethernet Switching Modules	
WS-X4124-FX-MT	24-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module
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
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
Ethernet/Fast Ethernet (10/100) Switching Modules	
WS-X4124-RJ45	24-port 10/100 RJ-45 module
WS-X4148-RJ	48-port 10/100 RJ-45 switching module
WS-X4148-RJ21	48-port 10/100 4xRJ-21 (telco connector) switching module
WS-X4148-RJ45V	48-port Pre-standard PoE 10/100BASE-T switching module
WS-X4224-RJ45V	24-port 10/100BASE-TX RJ-45 Cisco Catalyst 4500 series PoE 802.3af
WS-X4232-GB-RJ	32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet switching module

Table 1 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-E

Product Number (append with "=" for spares)	Product Description
WS-X4248-RJ45V	48-port 10/100BASE-T RJ-45 Cisco Catalyst 4500 series PoE 802.3af
WS-X4248-RJ21V	48-port 10/100 Fast Ethernet RJ-21 Cisco Catalyst 4500 series PoE 802.3af telco
WS-X4232-RJ-XX	32-port 10/100 Fast Ethernet RJ-45 modular uplink switching module
Small Form-Factor Pluggable 100 Megabit Ethernet Modules	
GLC-FE-100LX	100BASE-LX, 1310 nm wavelength, 10 km over SMF
GLC-FE-100BX-D	100BASE-BX10-D, 1550 nm TX/1310 nm RX wavelength
GLC-FE-100BX-U	100BASE-BX10-U, 1310 nm TX/1550 nm RX wavelength
GLC-FE-100EX	100BASE-EX for Fast Ethernet SFP Ports
GLC-FE-100ZX	100BASE-ZX for Fast Ethernet SFP Ports
GLC-FE-100FX	100BASE-FX SFP for Fast Ethernet SFP ports
GLC-GE-100FX	100BASE-FX SFP for Gigabit Ethernet SFP ports
GLC-EX-SMD	100BASE-EX GE SFP ports
Small Form-Factor Pluggable Gigabit Ethernet Modules	
GLC-BX-D	100BASE-BX10-D small form-factor pluggable module
GLC-BX-U	100BASE-BX10-U small form-factor pluggable module
GLC-SX-MM	100BASE-SX small form-factor pluggable module
GLC-SX-MMD	100BASE-SX small form-factor pluggable module
GLC-LH-SM	100BASE-LX/LH small form-factor pluggable module
GLC-LH-SMD	100BASE-LX/LH small form-factor pluggable module with DOM support
GLC-ZX-SM	100BASE-ZX small form-factor pluggable module
GLC-T	100BASE-T small form-factor pluggable module
CWDM-SFP-xxxx	CWDM small form-factor pluggable module (See Table 2 on page 9 for a list of supported wavelengths.)
10 Gigabit Ethernet X2 Pluggable Modules	
X2-10GB-LR	10GBASE-LR X2 transceiver module for SMF, 1310-nm wavelength, SC duplex connector
X2-10GB-ER	10GBASE-ER X2 transceiver module for SMF, 1550-nm wavelength, SC duplex connector
X2-10GB-CX4	10GBASE-CX4 X2 transceiver module for CX4 cable, copper, Infiniband 4X connector
X2-10GB-LX4	10GBASE-LX4 X2 transceiver module for MMF, 1310-nm wavelength, SC duplex connector
X2-10GB-LRM	10GBASE-LRM X2 transceiver module for MMF, 1310-nm wavelength, SC duplex connector
X2-10GB-SR	10GBASE-SR X2 transceiver module for MMF, 850-nm wavelength, SC duplex connector
X2-10GB-T	10GBASE-T X2 transceiver module, up to 100m wavelength on CAT6A or CAT7 copper cables
X2-10GB-ZR	10GBASE-ZR X2 transceiver module for SMF, 1550 nm wavelength up to 80 km. DOM is not supported.
X2-10GB-DWDM	10GBASE-ZR X2 transceiver module for SMF, 32 nontunable ITU 100-GHz wavelengths up to 80 km are supported. DOM is supported. Dual SC/PC connectors are supported.

Table 1 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-E

Product Number (append with “=” for spares)	Product Description
CVR-X2-SFP10G	Hot-swappable input/output (I/O) converter module that fits into a 10-Gigabit Ethernet X2 slot on a switch or line card module. Hosts one 10-Gigabit Ethernet SFP+ transceiver module.
SFP+ Modules	
SFP-10G-SR	Cisco 10GBASE-SR SFP+ Module for MMF
SFP-10G-LR	Cisco 10GBASE-LR SFP+ Module for SMF
SFP-10G-LRM	Cisco 10GBASE-LRM SFP+ Module for MMF
SFP-H10GB-CU1M	10GBASE-CU SFP+ Cable 1 Meter
SFP-H10GB-CU3M	10GBASE-CU SFP+ Cable 3 Meter
SFP-H10GB-CU5M	10GBASE-CU SFP+ Cable 5 Meter
SFP-10G-ER	Cisco 10GBASE-ER SFP+ Module for SMF
SFP-10G-ZR	Cisco 10GBASE-ZR SFP+ Module for SMF
Gigabit Interface Converter	
WS-G5483=	1000BASE-T GBIC
WS-G5484	1000BASE-SX short wavelength GBIC (multimode only)
WS-G5486	1000BASE-LX/LH long-haul GBIC (single mode or multimode)
WS-G5487	1000BASE-ZX extended reach GBIC (single-handed)
CWDM-GBIC-xxxx	CWDM gigabit interface converter (See Table 2 on page 9 for a list of supported wavelengths.)
DWDM-GBIC-xx.yy	Dense Wavelength-Division Multiplexing ITU 100-Ghz grid 15xx.yy nm GBIC.
WDM-GBIC-REC	Receive-only 1000BASE-WDM GBIC
Other Modules	
MEM-X45-2GB-E	SD Card, 2G
USB-X45-4GB-E	USB Thumb Drive, 4G
PWR-C45-1000AC	Catalyst 4500 series switch 1000 Watt AC power supply for chassis 4503, 4506, and 4507R (data only)
PWR-C45-1400DC	Catalyst 4500 series switch 1400 Watt DC triple input power supply (data-only)
PWR-C45-1400DC-P	Catalyst 4500 series switch 1400 Watt DC power supply with integrated PEM
PWR-C45-1400AC	Catalyst 4500 series switch 1400 Watt AC power supply (data-only)
PWR-C45-1300ACV	Catalyst 4500 series switch 1300 Watt AC power supply with integrated voice for chassis 4503, 4506, and 4507R
PWR-C45-2800ACV	Catalyst 4500 series switch 2800 Watt AC power supply with integrated voice (data and PoE) for chassis 4503, 4506, and 4507R
PWR-C45-4200ACV	Catalyst 4500 series switch 4200 Watt AC dual input power supply with integrated voice (data and PoE)
WS-P4502-1PSU	Catalyst 4500 series switch auxiliary power shelf (25-slot), including one PWR-4502
PWR-4502	Catalyst 4500 series switch auxiliary power shelf redundant power supply

Table 1 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-E

Product Number (append with “=” for spares)	Product Description
PWR-C45-6000ACV	Catalyst 4500 Series Switch 6000 W AC power supply
PWR-C45-9000ACV	Catalyst 4500 Series Switch 9000 W AC power supply

[Table 2](#) briefly describes the supported CWDM wavelengths in the Catalyst 4500E Series Switch.

Table 2 CWDM GBIC and SFP Supported Wavelengths on Cisco Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-E

Product Number (append with “=” for spares)	Product Description
CWDM-GBIC (or SFP) -1470	Longwave 1470 nm laser single-mode
CWDM-GBIC (or SFP) -1490	Longwave 1490 nm laser single-mode
CWDM-GBIC (or SFP) -1510	Longwave 1510 nm laser single-mode
CWDM-GBIC (or SFP) -1530	Longwave 1530 nm laser single-mode
CWDM-GBIC (or SFP) -1550	Longwave 1550 nm laser single-mode
CWDM-GBIC (or SFP) -1570	Longwave 1570 nm laser single-mode
CWDM-GBIC (or SFP) -1590	Longwave 1590 nm laser single-mode
CWDM-GBIC (or SFP) -1610	Longwave 1610 nm laser single-mode

[Table 3](#) briefly describes the supported DWDM wavelengths in the Catalyst 4500E Series Switch.

Table 3 DWDM SFP Supported Wavelengths on Cisco Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-E

Product Number (append with “=” for spares)	Product Description
DWDM-SFP-6061=	Cisco 1000BASE-DWDM SFP 1560.61 nm
DWDM-SFP-5979=	Cisco 1000BASE-DWDM SFP 1559.79 nm
DWDM-SFP-5898=	Cisco 1000BASE-DWDM SFP 1558.98 nm
DWDM-SFP-5817=	Cisco 1000BASE-DWDM SFP 1558.17 nm
DWDM-SFP-5655=	Cisco 1000BASE-DWDM SFP 1556.55 nm
DWDM-SFP-5575=	Cisco 1000BASE-DWDM SFP 1555.75 nm
DWDM-SFP-5413=	Cisco 1000BASE-DWDM SFP 1554.13 nm
DWDM-SFP-5494=	Cisco 1000BASE-DWDM SFP 1554.94 nm
DWDM-SFP-5252=	Cisco 1000BASE-DWDM SFP 1552.52 nm
DWDM-SFP-5172=	Cisco 1000BASE-DWDM SFP 1551.72 nm
DWDM-SFP-5092=	Cisco 1000BASE-DWDM SFP 1550.92 nm
DWDM-SFP-5012=	Cisco 1000BASE-DWDM SFP 1550.12 nm

Table 3 DWDM SFP Supported Wavelengths on Cisco Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-E

Product Number (append with “=” for spares)	Product Description
DWDM-SFP-4851=	Cisco 1000BASE-DWDM SFP 1548.51 nm
DWDM-SFP-4772=	Cisco 1000BASE-DWDM SFP 1547.72 nm
DWDM-SFP-4692=	Cisco 1000BASE-DWDM SFP 1546.92 nm
DWDM-SFP-4612=	Cisco 1000BASE-DWDM SFP 1546.12 nm
DWDM-SFP-4453=	Cisco 1000BASE-DWDM SFP 1544.53 nm
DWDM-SFP-4373=	Cisco 1000BASE-DWDM SFP 1543.73 nm
DWDM-SFP-4694=	Cisco 1000BASE-DWDM SFP 1542.94 nm
DWDM-SFP-4614=	Cisco 1000BASE-DWDM SFP 1542.14 nm
DWDM-SFP-4056=	Cisco 1000BASE-DWDM SFP 1540.56 nm
DWDM-SFP-3977=	Cisco 1000BASE-DWDM SFP 1539.77 nm
DWDM-SFP-3898=	Cisco 1000BASE-DWDM SFP 1539.98 nm
DWDM-SFP-3819=	Cisco 1000BASE-DWDM SFP 1538.19 nm
DWDM-SFP-3661=	Cisco 1000BASE-DWDM SFP 1536.61 nm
DWDM-SFP-3582=	Cisco 1000BASE-DWDM SFP 1535.82 nm
DWDM-SFP-3504=	Cisco 1000BASE-DWDM SFP 1535.04 nm
DWDM-SFP-3425=	Cisco 1000BASE-DWDM SFP 1534.25 nm
DWDM-SFP-3268=	Cisco 1000BASE-DWDM SFP 1532.68 nm
DWDM-SFP-3190=	Cisco 1000BASE-DWDM SFP 1531.90 nm
DWDM-SFP-3112=	Cisco 1000BASE-DWDM SFP 1531.12 nm
DWDM-SFP-3033=	Cisco 1000BASE-DWDM SFP 1530.33 nm

For details on DOM support for the Catalyst 4500E Series switches, refer to this URL:

http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6981.html#wp142660

Supported E Series Hardware on Cisco IOS XE Release 3.4.0SG

A brief list of primary E-Series hardware supported by Cisco IOS XE Release 3.4.0SG is shown in [Table 4](#).

Table 4 Supported E-Series Hardware

Product Number	Description
WS-C4503-E	Cisco Catalyst 4500E Series 3-Slot Chassis <ul style="list-style-type: none"> • Fan tray • No Power Supply
WS-C4506-E	Cisco Catalyst 4500E Series 6-Slot Chassis <ul style="list-style-type: none"> • Fan tray • No Power Supply
WS-C4507R-E	Cisco Catalyst 4500E Series 7-Slot Chassis <ul style="list-style-type: none"> • 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 4500E Series 7-Slot 48 GB-ready Chassis <ul style="list-style-type: none"> • 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 4500E Series 10-Slot Chassis <p>Note This chassis does not support the Supervisor Engine 7L-E.</p> <ul style="list-style-type: none"> • 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.
WS-C4510R+E	Cisco Catalyst 4500E Series 10-Slot 48 GB-ready Chassis <p>Note This chassis does not support the Supervisor Engine 7L-E.</p> <ul style="list-style-type: none"> • 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.

Feature Support by Image Type

Table 5 is a detailed list of features supported on Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-E running Cisco IOS XE Software Release 3.4.0SG categorized by image type. Please visit Feature Navigator for package details:

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

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

Feature	LAN Base	IP Base	Enterprise Services
2-way Community Private VLANs	No	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
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 QoS	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 and Supervisor Engine 7L-E

Feature	LAN Base	IP Base	Enterprise Services
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
Boot Config	Yes	Yes	Yes
Broadcast/Multicast Suppression	Yes	Yes	Yes
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

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

Feature	LAN Base	IP Base	Enterprise Services
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
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
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	No	Yes	Yes
Configuration Change Tracking Identifier	Yes	Yes	Yes
Configuration Change Notification and Logging	No	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
Configuration Replace and Configuration Rollback	Yes	Yes	Yes
Configuration Rollback Confirmed Change	Yes	Yes	Yes
Contextual Configuration Diff Utility	Yes	Yes	Yes
Control Plane Policing (Copp)	Yes	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
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
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
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
EIGRP	No	No	Yes
EIGRP Service Advertisement Framework	Yes	Yes	Yes
EIGRP Stub Routing	No	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
Embedded Event Manager (EEM) 3.2	No	Yes	Yes
Embedded Syslog Manager (ESM)	Yes	Yes	Yes
EnergyWise 2.5	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
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
Flexible NetFlow - Full Flow support	No	Yes	Yes
Flexible NetFlow - Ingress support	No	Yes	Yes
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 - NetFlow v5 Export Protocol	No	Yes	Yes
Flexible NetFlow - NetFlow v9 Export Format	No	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
Flexible NetFlow - VLAN ID support	No	Yes	Yes
Flex Links+ (VLAN Load balancing)	Yes	Yes	Yes
Forced 10/100 Autonegotiation	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
HSRP - Hot Standby Router Protocol	No	Yes	Yes
HSRPv2 for IPv6 Global Address Support	No	Yes	Yes
HTTP Security	Yes	Yes	Yes
HTTP TACAC+ Accounting support	Yes	Yes	Yes
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 ¹	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

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

Feature	LAN Base	IP Base	Enterprise Services
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
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

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

Feature	LAN Base	IP Base	Enterprise Services
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
IOS Based Device Profiling	No	Yes	Yes
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 - 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

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

Feature	LAN Base	IP Base	Enterprise Services
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	No	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
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 Routing: Static Hosts/Default Gateway	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 Lightweight DHCPv6 Relay Agent IPv6 Destination Guard IPv6 Snooping IPv6 Neighbor Discovery Multicast Suppression IPv6 Router Advertisement (RA) Guard	Yes	Yes	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-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 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
IPv6 Multicast: RPF Flooding of Bootstrap Router (BSR) Packets	No	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
IPv6 Multicast: Scope Boundaries	No	Yes	Yes
IPv6 Neighbor Discovery Duplicate Address Detection	Yes	Yes	Yes
IPv6 OSPFv3 NSF/SSO	No	Yes ²	Yes
IPv6 OSPFv3 Fast Convergence	No	Yes ²	Yes
IPv6 PACL	Yes	Yes	Yes
IPv6 RA Guard (Host Mode)	Yes	Yes	Yes
IPv6 Routing - EIGRP Support	No	No	Yes
IPv6 Routing: OSPF for IPv6 (OSPFv3)	No	Yes ²	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 Switching: CEF Support	No	Yes	Yes
IPv6 Switching: CEFv6 Switched Automatic IPv4-compatible Tunnels (in software)	No	Yes	Yes
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

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

Feature	LAN Base	IP Base	Enterprise Services
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
Layer 2 Control Packet	Yes	Yes	Yes
Layer 2 Protocol Tunneling (L2PT)	No	Yes	Yes
Layer 2 Traceroute	No	Yes	Yes
Layer 3 Multicast Routing (PIM SM, SSM, Bidir)	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
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

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

Feature	LAN Base	IP Base	Enterprise Services
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
NAC - L2 IEEE 802.1x	Yes	Yes	Yes
NAC - L2 IP	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) primary (formerly known as Network Time Protocol (NTP) master)	Yes	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
NMSP Enhancements <ul style="list-style-type: none"> • 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
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
Onboard Failure Logging (OBFL)	Yes	Yes	Yes
OSPF	No	Yes ²	Yes
OSPF v3 Authentication	No	Yes ²	Yes
OSPF Flooding Reduction	No	Yes ²	Yes
OSPF for Routed Access	No	Yes	Yes
OSPF Incremental Shortest Path First (i-SPF) Support	No	Yes ²	Yes
OSPF Link State Database Overload Protection	No	Yes ²	Yes
OSPF Not-So-Stubby Areas (NSSA)	No	Yes ²	Yes
OSPF Packet Pacing	No	Yes ²	Yes
OSPF Shortest Paths First Throttling	No	Yes ²	Yes
OSPF Stub Router Advertisement	No	Yes ²	Yes
OSPF Support for Fast Hellos	No	Yes ²	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
OSPF Support for Link State Advertisement (LSA) Throttling	No	Yes ²	Yes
OSPF Support for Multi-VRF on CE Routers	No	Yes ²	Yes
OSPF Update Packet-Pacing Configurable Timers	No	Yes ²	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
PIM Version 1	No	Yes	Yes
PIM Version 2	No	Yes	Yes
PoEP via LLDP	Yes	Yes	Yes
Policy Based Routing (PBR)	No	No	Yes
Policy-Based Routing (PBR) Recursive Next Hop	No	No	Yes
Port Security	Yes (supports 1024 MACs)	Yes (supports 3072 MACs)	Yes (supports 3072 MACs)s
Port Security on Etherchannel Trunk Port	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

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

Feature	LAN Base	IP Base	Enterprise Services
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 (Rapid-PVST)	Yes	Yes	Yes
Reduced MAC Address Usage	Yes	Yes	Yes
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
Secure Copy (SCP)	Yes	Yes	Yes
Secure Shell SSH Version 1 Integrated Client	Yes	Yes	Yes
Secure Shell SSH Version 1 Server Support	Yes	Yes	Yes
Secure Shell SSH Version 2 Client Support	Yes	Yes	Yes
Secure Shell SSH Version 2 Server Support	Yes	Yes	Yes
Single Rate 3-Color Marker for Traffic Policing	Yes	Yes	Yes
Smart Install Director Support ³	Yes	Yes	Yes
Smart Port	Yes	Yes	Yes
SNMP (Simple Network Management Protocol)	Yes	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
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
Source Specific Multicast (SSM) Mapping	No	Yes	Yes
SPAN (# of sessions) – Port Mirroring	Yes (4 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	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Loop Guard	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Portfast	Yes	Yes	Yes
Spanning Tree Protocol (STP) - PortFast BPDU Filtering	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Portfast BPDU Guard	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Portfast Support for Trunks	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Root Guard	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Uplink Fast Convergence	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Uplink Load Balancing	Yes	Yes	Yes
Spanning Tree Protocol (STP) Extension	Yes	Yes	Yes
Stateful Switchover	No	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
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 - Per-Port Multicast Suppression	Yes	Yes	Yes
STP Syslog Messages	Yes	Yes	Yes
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) ⁴	No	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
TrustSec: IEEE 802.1ae MACSec Layer 2 encryption	No	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
TrustSec: IEEE 802.1ae MACSec encryption on user facing ports	No	Yes	Yes
TrustSec: IEEE 802.1ae MACSec encryption on user facing ports SSO	No	Yes	Yes
TrustSec: IEEE 802.1ae MACSec encryption between switch-to-switch links using Cisco SAP (Security Association Protocol)	No	Yes	Yes
TrustSec SGT Exchange Protocol (SXP) IPv4	No	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
Virtual Router Redundancy Protocol (VRRP) for IPv4	No	Yes	Yes
Virtual Switching System (VSS) ⁵	No	Yes (SUP7E only)	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
VRF-aware TACACS+	No	No	Yes
VTP (Virtual Trunking Protocol) Version 2	Yes	Yes	Yes
VTP Version 3	Yes	Yes	Yes
WCCP Version 2	No	Yes	Yes
Web Authentication Proxy	Yes	Yes	Yes
Webauth Enhancements	Yes	Yes	Yes
Wireshark-based Ethernet Analyzer	No	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
XML-PI	Yes	Yes	Yes

1. IEEE 802.1t—An IEEE amendment to IEEE 802.1D that includes extended system ID, long path cost, and PortFast.
2. IP Base supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 200 dynamically learned routes.
3. Smart Install Director is not supported with VSS.
4. TDR is not supported on 46xx linecards.
5. Older generation line cards are not supported in the 3.4.0SG release with the VSS feature. These include all line cards starting with the 'WS-X45xy' id, and lower. 'WS-X44xy' and 'WS-X42xy' are some other examples of unsupported line cards. Please remove these line cards from your system when converting from standalone to VSS mode.

MIB Support

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

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

Features Not Supported on the Cisco Catalyst 4500E Series Switch

The following features are not supported on a Catalyst 4500E 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

Orderable Product Numbers

Table 6 Cisco IOS XE Software Release 3.4.0SG Product Numbers and Images for the Catalyst 4500E Series Switch

Product Number	Description	Image
S45EU-34-1512SG	CAT4500e SUP7-E/SUP7L-E Universal Image	cat4500e-universal.SPA.03.04.00.SG.151-2.SG.bin
S45EUK9-34-1512SG	CAT4500e SUP7-E/SUP7L-E Universal Crypto Image	cat4500e-universalk9.SPA.03.04.00.SG.151-2.SG.bin
S45EUN-34-1512SG	CAT4500e SUP7-E/SUP7L-E Universal No MACSEC Image	cat4500e-universalk9npe.SPA.03.04.00.SG.151-2.SG.bin
C4500E-LIC=	Base product ID for paper delivered software licenses	NA
C4500E-LB	LAN BASE software license (paper delivery)	NA
C4500E-IPB	IP BASE software license (paper delivery)	NA
C4500E-LB-IPB	LAN BASE to IP BASE upgrade license (paper delivery)	NA
C4500E-LB-ES	LAN BASE to Enterprise Services upgrade license (paper delivery)	NA
C4500E-IP-ES	IP BASE to Enterprise Services upgrade license (paper delivery)	NA
C4500E-LIC-PAK	Base product ID for paper delivered software licenses for spare Supervisor Engine 7-E	NA
C4500E-IP-ES-S	IP BASE to Enterprise Services upgrade license for spare Supervisor Engine7-E(paper delivery)	NA
C4500E-IPB-S	IP BASE software license for spare Supervisor Engine 7-E (paper delivery)	NA
L-C4500-LIC=	Base product ID for electronically delivered software licenses	NA
L-C4500E-LB-IP	LAN BASE to IP BASE upgrade license (electronically delivered)	NA
L-C4500E-IP-ES	IP BASE to Enterprise Services upgrade license (electronically delivered)	NA

Table 6 *Cisco IOS XE Software Release 3.4.0SG Product Numbers and Images for the Catalyst 4500E Series Switch*

Product Number	Description	Image
L-C4500E-LB-ES	LAN BASE to Enterprise Services upgrade license (electronically delivered)	NA

New and Changed Information

These sections describe the new and changed information for the Catalyst 4500 series switch running Cisco IOS software:

- [New Software Features in Release IOS XE 3.4.2SG, page 33](#)
- [New Hardware Features in Release IOS XE 3.4.2SG, page 33](#)
- [New Software Features in Release IOS XE 3.4.0SG, page 33](#)
- [New Hardware Features in Release IOS XE 3.4.0SG, page 34](#)

New Software Features in Release IOS XE 3.4.2SG

Release IOS XE 3.4.2SG provides the following new software on Catalyst 4500 Series switches:

- Permanent Right-to-Use (PRTU) license

New Hardware Features in Release IOS XE 3.4.2SG

Release IOS XE 3.4.0SG provides no new hardware on Catalyst 4500 Series switches.

New Software Features in Release IOS XE 3.4.0SG

Release IOS XE 3.4.0SG provides the following new software on Catalyst 4500 Series switches:

High Availability

- Virtual Switching System (VSS)
- ISSU—IPv4 Multicast
- ISSU—IPv6 Multicast
- NSF/SSO—IPv4 Multicast
- NSF/SSO—IPv6 Multicast

Security

- IPv6 First Hop Security
 - DHCPv6 Guard
 - Lightweight DHCPv6 Relay Agent (LDRA)
 - IPv6 Destination Guard

- IPv6 Snooping
- IPv6 Neighbor Discovery Multicast Suppression
- IPv6 Router Advertisement (RA) Guard
- Other
 - Reverse SSH Enhancements
 - Secure Shell SSH Version 2 Client Support
 - Secure Shell SSH Version 2 Server Support
 - SSH Keyboard Interactive Authentication
 - SSHv2 Enhancements
 - SSHv2 Enhancements for RSA Keys

Lower Total Cost of Ownership and Ease of Use

- Smart Install (Director Support)

Routing and Multicast Enhancements

- BGP Consistency Checker
- IPv6 BSR Scoped Zone support
- OSPFv3 Address Families
- OSPFv3 Time To Live Security
- Policy Based Routing: Recursive Next Hop

IPv6 Access Control

- IPv6 VACL (Vlan Access Control List)
- SPAN ACL Filtering for IPv6

Other

- FTP IPv6 Support
- IPSLA 4.0 - IPv6 phase 2
- IPSLA Multicast Support
- NTPv4 Orphan Mode support, Range for trusted key configuration
- TFTP IPv6 Support
- WSMA and XMLPI enhancement

New Hardware Features in Release IOS XE 3.4.0SG

Release IOS XE 3.4.0SG provides the following new hardware on Catalyst 4500 Series switches:

- X2-10GB-T for 10GBASE-T X2 Support—Provides link lengths up to 100m on CAT6A or CAT7 copper cables

Cisco IOS XE to Cisco IOS Version Number Mapping

As [Table 7](#) shows, each version of Cisco IOS XE has an associated Cisco IOS version:

Table 7 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOS 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

Upgrading the System Software

If you are upgrading to Cisco IOS XE Version 3.4.0SG and are planning on using VSS, you must upgrade your ROMMON to IOS Version 15.0(1r)SG7. Otherwise, you must upgrade your ROMMON to at least IOS Version 15.0(1r)SG2.

Be aware that you can upgrade a ROMMON image either through a console or telnet.

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

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

This section lists the limitations and restrictions for the current release of Cisco IOS software on the Catalyst 4500E series switch.

- Starting with Release IOS XE 3.3.0SG and IOS 15.1(1)SG, the seven RP restriction was removed.
- 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.

- 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.ffe0 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.ffe0 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 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

- When sup1 is in ROMMON and sup2 is in IOS, only sup2 can read the SEEPROM contents of the following chassis components:

- chassis
- fan-tray
- clock-module
- power-supplies
- mux-buffer for each linecard slot
- linecards

On sup1, when the **sprom read ..** command is entered for any of the above components, the SEEPROM contents are displayed as all “0”s.

When sup1 and sup2 are both in ROMMON (or both in IOS (SSO state)), they can read all SEEPROMs.

- 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

- When you connect two PoE-capable Catalyst 4648 or 4748 modules with straight-through copper cabling, the link may flap, and you may observe incorrect PoE status. If the port belongs to an EtherChannel, it will repeatedly unbundle, then bundle.

Workarounds:

- Use a crossover cable.

- Enter the **diagnostic dpm-discovery-disable module m** command provided you are running Cisco IOS XE Release 3.4.1SG or higher. CSCub74707
- Auto negotiation cannot be disabled on the Fa1 port. It must be set to auto/auto, or fixed speed with duplex auto.
- When performing an ISSU upgrade from a release prior to Cisco IOS 15.1(2)SG to release Cisco IOS 15.1(2)SG or higher, dynamic ACLs are lost after the first switchover.
Workaround: Enter **shut** then **no shut** on any port to restart the authentication session and restore the ACL. CSCul20163
- When performing an ISSU between any releases prior to Cisco IOS 15.1(1)SG or 3.3.0SG to release Cisco IOS 15.1(1)SG (or 3.3.0SG) or higher, a switch performing multicast routing may persistently drop traffic after the upgrade completes. You can recover multicast traffic by reloading the chassis. Alternately, you can remove all multicast configuration prior to ISSU, and add it back when ISSU completes. CSCuj42672

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.



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

Cisco Bug Search Tool

The Bug Search Tool (BST) is the online successor to Bug Toolkit and 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. You can access the tool at: <https://tools.cisco.com/bugsearch/>.

To view the details of a caveat listed in this document:

1. Click on the link in the **Bug ID** column.
2. Logon to the BST using your Cisco user ID and password

Resolved Caveats for Cisco IOS XE Release 3.4.9 SG

Bug ID	Headline
CSCup70353	Cisco IOS XE Software Web User Interface Denial of Service Vulnerability

Resolved Caveats for Cisco IOS XE Release 3.4.8 SG

Bug ID	Headline
CSCux65501	4500X forwards Ethernet I frames on stp blocked port
CSCuz10028	ACLHWPROGERR message seen with IPV6 ACL+L4 operator
CSCuy82367	Cisco IOS and IOS XE Software Smart Install Memory Leak Vulnerability
CSCuy92401	Texel SG6: CTS periodic reviews are started at portBringup
CSCuw17135	Cat4k SUP7L-E CPU temperature sensor failed
CSCuz26852	Interrupts for Parity Error are not enabled after 'reload' command.
CSCva10393	system crashed during boot up on 4948E
CSCuv14614	WS-X4640-CSFP-E ports (Tx) are disabled
CSCur20842	multiple match criteria should not be allowed on EC member ports
CSCur03797	policy-map with policer percent/DBL results in non-sharing of TCAM entry
CSCuu43892	switch crash on qpair_full after executing dhcpd_* functions
CSCup90532	Cisco IOS and IOS XE Software DNS Forwarder Denial of Service Vulnerability
CSCux82995	AmurMR4: EPM ACL Plugin process memory holding increases with CoA
CSCuv03066	Switch crashed
CSCuw48118	ASR920 - crash in bcopy called from 'addnew' during reassembly
CSCux66005	Cisco IOS XE Software IP Fragment Reassembly Denial of Service Vuln.
CSCud36767	Cisco IOS and IOS XE MSDP SA Message Denial of Service Vulnerability
CSCum36951	Cisco IOS Software IKEv2 Denial of Service Vulnerabilities
CSCvb29204	BenignCertain on IOS and IOS-XE
CSCuy47382	Cisco IOS and IOS XE Software IKEv1 1 Fragmentation Denial of Service Vulnerability
CSCuw85826	Evaluation of Cisco IOS and IOS-XE for NTP_October_2015
CSCux46898	NTP associations vulnerability
CSCum19502	Inconsistent behavior between telnet and ssh in low memory conditions
CSCva37519	stale flowmgr entry during ipv6 tacacs transaction leads to crash
CSCuy38709	Memory leak with watcher_create_common.
CSCvb16274	PPTP Start-Control-Connection-Reply packet leaks router memory contents

Open Caveats for Cisco IOS XE Release 3.4.7SG

Bug ID	Headline
--------	----------

CSCui10480	UDE does not work properly
CSCuc49150	You cannot detach an input QoS policy from VSL member ports

Resolved Caveats for Cisco IOS XE Release 3.4.7SG

Bug ID	Headline
CSCus19794	Cisco IOS and IOS XE IPv6 SEND Denial of Service Vulnerability
CSCus21950	Crash seen after getting LINEPROCDEAD errors and tracebacks
CSCuu90695	DM/SM boundary (S,G) are not repopulated: Multicast Missing Registration
CSCul01067	Memory leak in NTP client with IPv6 configuration
CSCuq66263	Switch crashes when ACL add entry
CSCuq53377	AAA AttrL memory Leak due to Auth-Manager
CSCuq24202	Cisco IOS TCL script interpreter privilege escalation vulnerability
CSCut87425	CPU hog in "EEM TCL Proc" after TCL script termination with long runtime
CSCuu77313	4948 - rxSymbolErrors and rxSequenceErrors incrementing

Open Caveats for Cisco IOS XE Release 3.4.6SG

Bug ID	Headline
CSCts26844	Disparity btwn Cisco TrustSec and RADIUS accounting
CSCts20229	Mediatrace cannot find the correct inbound interface
CSCtx51561	Problem with adding "bfd" suffix to the snmp server host
CSCuc36612	Error-disable event in a multichassis port channel on a VSS system
CSCud39208	Error messages and traceback for Bidir PIM
CSCui10480	UDE does not work properly
CSCto46018	Device in a guest VLAN has packet loss after a SSO failover
CSCuc49150	You cannot deattach an input QoS policy from VSL member ports
CSCun83237	On VSS active switch, devices cannot reach the internet or server

Resolved Caveats for Cisco IOS XE Release 3.4.6SG

Bug ID	Headline
CSCtf75400	Wrong output for show platform software etherchannel port-channel n map
CSCuf52741	file verify auto always present in default-running-config
CSCug90126	C4510 returns incorrect ciscoEnvMonSupplyState value
CSCul73513	Clock is not matching between server-client after leap configuration

CSCum56902	Sup7L-E FFM Crashes while removing the class-map
CSCun34745	"ip ssh source-interface" configuration missing after reload
CSCuo26294	Switch crashes with process FFM terminated abnormally
CSCuo28455	SMI - Custom group doesn't work for new PIDS not in the IBD database
CSCup84251	Crash on purge_app_tlv_and_notify
CSCuq01267	HSRP VMAC is not programmed after SSO in cat4k VSS setup
CSCuq04574	WS-C4500X-16 with 3.5.3E crashes due to SNMP polling
CSCuq80812	Incomplete ARP reply received on an active Flex Link port
CSCur21848	WCCP stops redirecting traffic when eighth port added to service group
CSCur23656	Cisco IOS and IOSd in IOS-XE : evaluation of SSLv3 POODLE vulnerability
CSCur84243	WS-X4640-CSFP-E ports (Tx) are disabled on start-up
CSCur98467	VSL-MGMT access-list mac address changes after entire VSS reload
CSCus23266	C4500X deny ACE does not work correctly
CSCus47714	VSS active and standby MAC address table can not synchronisation issue.
CSCus69731	IOS-XE for Nova device: glibc GHOST vulnerability - CVE-2015-0235

Open Caveats for Cisco IOS XE Release 3.4.5SG

Bug ID	Headline
CSCts26844	Disparity btwn Cisco TrustSec and RADIUS accounting
CSCts20229	Mediatrace cannot find the correct inbound interface
CSCtx51561	Problem with adding "bfd" suffix to the snmp server host
CSCuc36612	Error-disable event in a multichassis port channel on a VSS system
CSCud39208	Error messages and traceback for Bidir PIM
CSCui10480	UDE does not work properly
CSCto46018	Device in a guest VLAN has packet loss after a SSO failover
CSCuc49150	You cannot deattach an input QoS policy from VSL member ports
CSCuo18934	After ISSU to 3.2.7, multicast packet loss is observed
CSCun83237	On VSS active switch, devices cannot reach the internet or server
CSCtg00542	LACP delay with netflow sampling

Resolved Caveats for Cisco IOS XE Release 3.4.5SG

Bug ID	Headline
CSCsl41325	Device crashes when a routing adjacency goes down; spurious memory access
CSCse19848	Multicast and broadcast SNMP counters are not populated for some interf.

CSCse78880	ACL config. sync. error: Line-by-line sync. verification failure
CSCts88778	Incorrect usage of sstrncpy() in "qnq_switch_cli.c" file
CSCuc03836	Switch reports SYS-2-MALLOCFAIL error for a very large amount of memory
CSCuc81286	Entering the "show spi-fc 12" cmd causes the device to crash
CSCud86438	Stack member memory leak in "HULC DOT1X Process"
CSCug17582	Message "Password required, but none set" after entering "enable" cmd
CSCug77784	File table overflow: private-config file open fails
CSCui36462	Random interfaces stop receiving traffic
CSCui87789	Switch fails after entering the "clear ip dhcp conflict *" command
CSCuj66318	Vulnerability in NTP implmntn: allows query with access-group configured
CSCum54321	The switch crash file is not saved on certain IOS platforms
CSCum71764	VLAN intf. not ready when 'ip igmp mroute-proxy' configured after reboot
CSCum80951	TCAM does not share when same policy is applied to multiple interfaces
CSCum91811	Switching loop occurs when removing DTP from port-channel.
CSCun13984	The switch reloads while modifying static mac address-table entry
CSCun11927	OAM not working after link flap between 4500X and ASR9K
CSCun22906	Output drop on Ten port of C4948E with random size packet
CSCun55459	CVV VLAN Policy does not appear in "show auth sess" CLI output
CSCun92058	Memory leak @ *MDA context* after configuring dot1x auth
CSCuo26294	Switch crashes with process FFM terminated abnormally
CSCuo51767	REP preemption is not triggered with link state change
CSCuo73465	RPF not updated in hardware table
CSCuo80260	Call-home message fails; returns "Unknown" serial number
CSCuo88868	Link debounce config passes to port-channel after a flap on members
CSCuo89407	Problem with adding new ports to a channel group.
CSCuo90172	Software returns incorrect MIB value from day 1
CSCup06835	UDLD not working on a switch with port as dot1q trunk
CSCup08161	Stacklow crash when copying file via SNMP
CSCup22590	Multiple Vulnerabilities in IOS/IOSd OpenSSL - June 2014
CSCup39712	Switch crashes with critical software exception during config push
CSCup52101	EnergyWise Denial of Service vulnerabilty
CSCup71993	DOT1x issues while using "authentication open"
CSCuq02796	Catalyst 4500-X VSS failure after adding members to port-channel
CSCuq09636	Single bit error corrected on Sup7-E is inadvertently logged in syslog
CSCuq39071	Mcast packet loss when other receiver leaves group in IGMPv3
CSCur03368	IOS-XE for Nova devices: GNU Bourne Shell "Shellshock" Vulnerability"

Open Caveats for Cisco IOS XE Release 3.4.4SG

This section lists the open caveats for Cisco IOS XE Release 3.4.4SG:

- When you enable both Cisco TrustSec and RADIUS accounting, a disparity occurs between the RADIUS client (Cisco switch) and the RADIUS/CTS server in how the authenticator field in the header is computed for DOT1X/RADIUS accounting messages.

A Cisco IOS AAA client uses the PAC secret to compute the authenticator; Cisco Secure ACS 5.2 uses the shared secret. This behavior causes a mismatch that results in a rejection of the accounting message, and the client marks the server as unresponsive.

Workaround: None. You must disable 802.1X accounting. CSCts26844

- When more than one Equal Cost Multipath (ECMP) is available on the downstream switch, and Mediatrace is invoked to provide flow statistics, the dynamic policy does not show statistics for a flow.

Mediatrace cannot find the correct inbound interface and applies the dynamic policy on a different interface from the one used for media flow.

Workaround: None. CSCts20229

- When you add a "bfd" suffix to the **snmp server host** *x.x.x.x* configuration command, the BFD traps, ciscoBfdSessUp and ciscoBfdSessDown, are not generated.

Workaround: Do not specify a "bfd" suffix with the **snmp-server host** *x.x.x.x* configuration command. CSCtx51561

- In a multichassis port channel on a VSS system with a very high number of link up and down events that occur within a second and typically causes an error-disable event, only the ports on the active switch are error-disabled due to flaps.

Workaround: None. CSCuc36612

- The following (information-only) error message and traceback may occur during MFIB-to-platform state updates for Bidirectional PIM (*,G/m) entries associated with Bidirectional PIM rendezvous points:

```
%SYS-2-NOBLOCK: may_suspend with blocking disabled. -Process= "MFIB_mrib_read", ipl=
0, pid= 370
-Traceback= 1#f95b67f80cdf0886bbf15560d7553abc :152CC000+2699F4C :152CC000+269A310
:152CC000+1F1B55C :152CC000+38D5F4C :152CC000+2C25698 :152CC000+2C2EDF4
:152CC000+5F6F0B0 :152CC000+5F6F1A0 :152CC000+2C2F274 :152CC000+2C24AA4
:152CC000+119935C :152CC000+1D94244 :152CC000+119B070 :152CC000+119699C
:152CC000+2C50D00 :152CC000+2B5901C
```

These messages are typically observed during SSO, bootup, or when a PIM-enabled interface undergoes a state transition on a switch containing Bidir PIM state entries.

Workaround: None. CSCud39208

- Configuring an interface as unidirectional with the **unidirectional send-only | receive-only** command still allows an interface to send (configured as Send-only Unidirection Ethernet mode) or receive (configured as Receive-only Unidirection Ethernet mode) packets in a bidirectional mode.

Workaround: None. CSCui10480

- If you enter the **show spi-fc 12** command, a crash occurs.

Workaround: Use the **show spi-fc all** command to dump all SPI channel information. CSCuc81286

- You can attach an input QoS policy to VSL member ports, but you cannot detach it. You only can configure VSL ports.

Workaround: Default the VSL member ports and detach the input QoS policy. CSCuc49150

- A device in a guest VLAN that is connected behind a phone capable of 2nd-port-notification experiences packet loss following a SSO failover. The device experiences an authentication restart after the first CDP frame arrives from the phone.

Workaround: None. CSCto46018

- After performing an ISSU from Cisco IOS Release 3.2.3 to 3.2.7, multicast packet loss is observed after both supervisor engines are running IOS Release 3.2.7

Workaround: Do a switchover. CSCuo18934

- On a VSS active switch, devices (i.e., hosts, phones, or workstations) directly connected to ports Gi1/7/38, Gi1/7/39, Gi1/7/40, Gi1/7/43 on VLAN 34 cannot reach the internet or server.

Workaround: None. CSCun83237

- Occasionally, when netflow sampling is enabled, LACP requires about 60-70 sec until members are bundled.

Workaround: Disable netflow sampling. CSCtg00542

- Upon adding a new static MAC entry on a Catalyst 4500X VSS running version 3.4.3 and 3.5.x, the switch number is truncated in the running config. Although the entry functions as expected, it displays incorrectly. Upon reload, it encounters an error because the entry is no longer a valid switch, module, or port.

```
4500x_vss(config)#mac address-table static 03bf.ac10.0cb9 vlan 1 interface Te1/2/3
```

```
4500x_vss#show run | i mac add
```

```
mac address-table static 03bf.ac10.0cb9 vlan 1 interface Te2/3 <--- Missing the 1/
```

Upon reload, the config errors out

```
mac address-table static 03bf.ac10.0cb9 vlan 1 interface Te2/3
```

```
^
```

```
% Invalid input detected at '^' marker.
```

Workaround: After a reload, manually re-add the static entry into the running config. CSCuo60703

- A switch may crash due to an interaction with PIM.

The exact triggers are unknown.

Workaround: None. CSCuo37416

- When **ip igmp mroute-proxy** is configured and you reload the switch, it will remove the command:

```
interface Vlan14
 ip address 10.1.1.1 255.255.255.252
 ip pim sparse-mode
 ip igmp mroute-proxy Vlan2137
end
```

```
48 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.
```

```
ip igmp mroute-proxy Vlan2137
```

```
^
```

```
% Invalid input detected at '^' marker.
```

Workaround: Reapply the configuration when the switch reboots. CSCum71764

Resolved Caveats for Cisco IOS XE Release 3.4.4SG

This section lists the resolved caveats for Cisco IOS XE Release 3.4.4SG:

- When you configure open authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new Standby supervisor engine. This behavior interrupts traffic only after the second switchover because the new Standby supervisor engine possesses the wrong state after the initial switchover and the second switchover starts the port in the blocking state.
Workaround: Enter **shut** and **no shut** on the port to synchronize the STP state. CSCtf52437
- Packets that are routed on the same Layer 3 interface (or SVI) that entered on are dropped if received on the VSS standby switch.
Workaround: None. CSCuj67614
- A switch crashes on receiving a malformed LLDP packet.
LLDP should be enabled.
Workaround: None. CSCun66735
- Upon removing the active supervisor engine from a switch, multicast and unicast packet loss occur (for 60 seconds) until route convergence completes.
Workaround: None. CSCun97605

Open Caveats for Cisco IOS XE Release 3.4.3SG

This section lists the open caveats for Cisco IOS XE Release 3.4.3SG:

- When an SNMP query includes the cpmCPUProcessHistoryTable, the query time is very slow, and CPU utilization of the os_info_p process (OS Information provider) increases substantially. The query time of an almost fully populated table is 68 minutes.
Workaround: None. CSCth42248
- The **show ipv6 access-list** command displays incorrect match counts when multicast traffic is matched to an IPv6 access list that is attached to an SVI.
Workaround: None. CSCth65129
- When you configure open authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new Standby supervisor engine. This behavior interrupts traffic only after the second switchover because the new Standby supervisor engine possesses the wrong state after the initial switchover and the second switchover starts the port in the blocking state.
Workaround: Enter **shut** and **no shut** on the port to synchronize the STP state. CSCtf52437
- If you reboot a switch, the configured value of the interface MTU size for the elements of the port channel interface does not work for IPv6 traffic.
Workaround: After the switch reloads, enter **shut** and **no shut** on the port-channel interface. CSCto27085
- Dynamic buffer limiting might not function at queue limits less than or equal to 128.
Workaround: Increase the queue limit to at least 256. CSCto57602
- A device in a guest VLAN that is connected behind a phone capable of 2nd-port-notification experiences packet loss following a SSO failover. The device experiences an authentication restart after the first CDP frame arrives from the phone.

Workaround: None. CSCto46018

- If you perform an OIR on a line card, several %C4K_RKNOVA-4-INVALIDTOKENEXPIRED messages appear in the logs.

Workaround: None. CSCtu37959

- When you enable both Cisco TrustSec and RADIUS accounting, a disparity occurs between the RADIUS client (Cisco switch) and the RADIUS/CTS server in how the authenticator field in the header is computed for DOT1X/RADIUS accounting messages.

A Cisco IOS AAA client uses the PAC secret to compute the authenticator; Cisco Secure ACS 5.2 uses the shared secret. This behavior causes a mismatch that results in a rejection of the accounting message, and the client marks the server as unresponsive.

Workaround: None. You must disable 802.1X accounting. CSCts26844

- When more than one Equal Cost Multipath (ECMP) is available on the downstream switch, and Mediatrace is invoked to provide flow statistics, the dynamic policy does not show statistics for a flow.

Mediatrace cannot find the correct inbound interface and applies the dynamic policy on a different interface from the one used for media flow.

Workaround: None. CSCts20229

- When a switchover is created on the Mediatrace responder, the dynamic access list created for a monitored flow tuple is not deleted. Although the Mediatrace initiator creates another set of dynamic access lists after the switchover, the old ones remain in the configuration.

Stale dynamic access lists force the system to monitor unwanted traffic.

Workarounds:

- If the switchover is scheduled, remove the scheduled session on the initiator and reschedule the session after the new active supervisor engine boots on the responder.
- If the Mediatrace responder SSO is not planned, after the new active supervisor engine boots, manually delete the stale dynamic access lists. CSCty75070
- When you add a "bfd" suffix to the **snmp server host** *x.x.x.x* configuration command, the BFD traps, ciscoBfdSessUp and ciscoBfdSessDown, are not generated.

Workaround: Do not specify a "bfd" suffix with the **snmp-server host** *x.x.x.x* configuration command. CSCtx51561

- During either a system- or user-initiated reload operation, the following message is observed when the system shuts down:

```
HARDWARE WATCHDOG
```

This message is not observed during a system bootup.

Workaround: None required. This message is information only. CSCtz15738

- In a multichassis port channel on a VSS system with a very high number of link up and down events that occur within a second and typically causes an error-disable event, only the ports on the active switch are error-disabled due to flaps.

Workaround: None. CSCuc36612

- If you enter the **show spi-fc 12** command, a crash occurs.

Workaround: Use the **show spi-fc all** command to dump all SPI channel information. CSCuc81286

- When you enter the **ip pim register-rate-limit** command, the following error message displays:

'Failed to configure service policy on register tunnel' and 'STANDBY:Failed to configure service policy on register tunnel'.

Workaround: None. The **ip pim register-rate-limit** command does not function. CSCub32679

- Packets that are routed on the same Layer 3 interface (or SVI) that entered on are dropped if received on the VSS standby switch.

Workaround: None. CSCuj67614

- Ports occasionally stay down after an OIR of a standby line card in VSS.

Workaround: Enter **shut**, then **no shut** to bring up the links. CSCuc37676

- You can attach an input QoS policy to VSL member ports, but you cannot detach it. You only can configure VSL ports.

Workaround: Default the VSL member ports and detach the input QoS policy. CSCuc49150

- When VSS receives a VTP message with information about the creation of 4000 VLANs, traceback and syslog messages (containing EM-4-SEARCH) are displayed.

Workaround: None. You might try reducing the number of VLANs created at one time.

CSCuc66206

- For packets with the same ingress and egress Layer 3 interface, ingress QoS marking policy does not work.

Workaround: Turn off ICMP redirect through the **ip redirect** command. CSCua71929

- When the Wireshark feature is applied on a control panel, it fails to capture the correct packets as they travel to the CPU in VSS, under the following conditions:

- Incoming packets on the VSS standby port are directed to the CPU for host learning.
- Layer 3 exceptions occur for packets arriving on the VSS standby port.
- ACL logging occurs on the VSS standby port.

Workaround: None. CSCub33727

- The POST results on the VSS standby switch displayed by the **show diagnostic result module all detail** command indicate module number 1 rather than 11. The module number is not interpreted by Cisco IOS.

Workaround: None. CSCuc73632

- The following (information-only) error message and traceback may occur during MFIB-to-platform state updates for Bidirectional PIM (*,G/m) entries associated with Bidirectional PIM rendezvous points:

```
%SYS-2-NOBLOCK: may_suspend with blocking disabled. -Process= "MFIB_mrrib_read", ipl=
0, pid= 370
-Traceback= 1#f95b67f80cdf0886bbf15560d7553abc :152CC000+2699F4C :152CC000+269A310
:152CC000+1F1B55C :152CC000+38D5F4C :152CC000+2C25698 :152CC000+2C2EDF4
:152CC000+5F6F0B0 :152CC000+5F6F1A0 :152CC000+2C2F274 :152CC000+2C24AA4
:152CC000+119935C :152CC000+1D94244 :152CC000+119B070 :152CC000+119699C
:152CC000+2C50D00 :152CC000+2B5901C
```

These messages are typically observed during SSO, bootup, or when a PIM-enabled interface undergoes a state transition on a switch containing Bidir PIM state entries.

Workaround: None. CSCud39208

- Configuring an interface as unidirectional with the **unidirectional send-only | receive-only** command still allows an interface to send (configured as Send-only Unidirection Ethernet mode) or receive (configured as Receive-only Unidirection Ethernet mode) packets in a bidirectional mode.

Workaround: None. CSCui10480

Resolved Caveats for Cisco IOS XE Release 3.4.3SG

This section lists the resolved caveats for Cisco IOS XE Release 3.4.3SG:

- On systems performing multicast routing, a brief increase in CPU consumption occurs every few minutes. In large-scale environments, this CPU increase is more noticeable.
Workaround: None. CSCub44553
- Following a switchover on VSS, CPU may remain high. The **show platform cpu packet statistics** command displays high usage due to “SA Miss.”
Workaround: Clear the MAC table. CSCuh50329
- Frequent polling of CPU-PROCESS-MIB may cause a switch to unexpectedly reload.
Workaround: None.CSCug65204
- SNMP may time out and produce CPUHOG messages when lldpXMedMIB is polled.
Workaround: CSCuh88726
- A port configured for webauth is not programmed with the default or fallback ACL when sessions enter the INIT state.
Workaround: None. CSCuj71597
- When a device authenticates with dot1x after authenticating with MAB, any policies applied by MAB remain in place.
Workarounds:
 - Ensure that the dot1x supplicant always authenticates before MAB.
 - Create MAB policies for dot1x hosts that do not supply a URL redirect. CSCui79988
- On a Catalyst 4500 VSS using IOS Release XE 3.4.0SG to 3.4.2SG, or 3.5.0E, the **show platform** command may be truncated with a "Timed out" message and may rarely produce an unexpected reload. The likelihood of a reload increases if the command is issued over an SSH session or if the output is redirected to a file. The same behavior is observed using IOS Release XE 3.5.0 and the **show tech** command.
Workaround: None. CSCul00025

Open Caveats for Cisco IOS XE Release 3.4.2SG

This section lists the open caveats for Cisco IOS XE Release 3.4.2SG:

- When an SNMP query includes the cpmCPUProcessHistoryTable, the query time is very slow, and CPU utilization of the os_info_p process (OS Information provider) increases substantially. The query time of an almost fully populated table is 68 minutes.
Workaround: None. CSCth42248
- The **show ipv6 access-list** command displays incorrect match counts when multicast traffic is matched to an IPv6 access list that is attached to an SVI.
Workaround: None. CSCth65129

- When you configure open authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new Standby supervisor engine. This behavior interrupts traffic only after the second switchover because the new Standby supervisor engine possesses the wrong state after the initial switchover and the second switchover starts the port in the blocking state.

Workaround: Enter **shut** and **no shut** on the port to synchronize the STP state. CSCtf52437

- If you reboot a switch, the configured value of the interface MTU size for the elements of the port channel interface does not work for IPv6 traffic.

Workaround: After the switch reloads, enter **shut** and **no shut** on the port-channel interface. CSCto27085

- Dynamic buffer limiting might not function at queue limits less than or equal to 128.

Workaround: Increase the queue limit to at least 256. CSCto57602

- A device in a guest VLAN that is connected behind a phone capable of 2nd-port-notification experiences packet loss following a SSO failover. The device experiences an authentication restart after the first CDP frame arrives from the phone.

Workaround: None. CSCto46018

- If you perform an OIR on a line card, several %C4K_RKNOVA-4-INVALIDTOKENEXPIRED messages appear in the logs.

Workaround: None. CSCtu37959

- When you enable both Cisco TrustSec and RADIUS accounting, a disparity occurs between the RADIUS client (Cisco switch) and the RADIUS/CTS server in how the authenticator field in the header is computed for DOT1X/RADIUS accounting messages.

A Cisco IOS AAA client uses the PAC secret to compute the authenticator; Cisco Secure ACS 5.2 uses the shared secret. This behavior causes a mismatch that results in a rejection of the accounting message, and the client marks the server as unresponsive.

Workaround: None. You must disable 802.1X accounting. CSCts26844

- When more than one Equal Cost Multipath (ECMP) is available on the downstream switch, and Mediatrace is invoked to provide flow statistics, the dynamic policy does not show statistics for a flow.

Mediatrace cannot find the correct inbound interface and applies the dynamic policy on a different interface from the one used for media flow.

Workaround: None. CSCts20229

- When a switchover is created on the Mediatrace responder, the dynamic access list created for a monitored flow tuple is not deleted. Although the Mediatrace initiator creates another set of dynamic access lists after the switchover, the old ones remain in the configuration.

Stale dynamic access lists force the system to monitor unwanted traffic.

Workarounds:

- If the switchover is scheduled, remove the scheduled session on the initiator and reschedule the session after the new active supervisor engine boots on the responder.
 - If the Mediatrace responder SSO is not planned, after the new active supervisor engine boots, manually delete the stale dynamic access lists. CSCty75070
- When you add a "bfd" suffix to the **snmp server host** *x.x.x.x* configuration command, the BFD traps, `ciscoBfdSessUp` and `ciscoBfdSessDown`, are not generated.

Workaround: Do not specify a "bfd" suffix with the **snmp-server host** *x.x.x.x* configuration command. CSCtx51561

- During either a system- or user-initiated reload operation, the following message is observed when the system shuts down:

```
HARDWARE WATCHDOG
```

This message is not observed during a system bootup.

Workaround: None required. This message is information only. CSCtz15738

- In a multichassis port channel on a VSS system with a very high number of link up and down events that occur within a second and typically causes an error-disable event, only the ports on the active switch are error-disabled due to flaps.

Workaround: None. CSCuc36612

- If you enter the **show spi-fc 12** command, a crash occurs.

Workaround: Use the **show spi-fc all** command to dump all SPI channel information. CSCuc81286

- When you enter the **ip pim register-rate-limit** command, the following error message displays:

```
'Failed to configure service policy on register tunnel' and 'STANDBY:Failed to
configure service policy on register tunnel'.
```

Workaround: None. The **ip pim register-rate-limit** command does not function. CSCub32679

- Packets that are routed on the same Layer 3 interface (or SVI) that entered on are dropped if received on the VSS standby switch.

Workaround: None. CSCuj67614

- Ports occasionally stay down after an OIR of a standby line card in VSS.

Workaround: Enter **shut**, then **no shut** to bring up the links. CSCuc37676

- You can attach an input QoS policy to VSL member ports, but you cannot detach it. You only can configure VSL ports.

Workaround: Default the VSL member ports and detach the input QoS policy. CSCuc49150

- When VSS receives a VTP message with information about the creation of 4000 VLANs, traceback and syslog messages (containing EM-4-SEARCH) are displayed.

Workaround: None. You might try reducing the number of VLANs created at one time.

CSCuc66206

- For packets with the same ingress and egress Layer 3 interface, ingress QoS marking policy does not work.

Workaround: Turn off ICMP redirect through the **ip redirect** command. CSCua71929

- On systems performing multicast routing, a brief increase in CPU consumption occurs every few minutes. In large-scale environments, this CPU increase is more noticeable.

Workaround: None. CSCub44553

- When the Wireshark feature is applied on a control panel, it fails to capture the correct packets as they travel to the CPU in VSS, under the following conditions:

- Incoming packets on the VSS standby port are directed to the CPU for host learning.
- Layer 3 exceptions occur for packets arriving on the VSS standby port.
- ACL logging occurs on the VSS standby port.

Workaround: None. CSCub33727

- The POST results on the VSS standby switch displayed by the **show diagnostic result module all detail** command indicate module number 1 rather than 11. The module number is not interpreted by Cisco IOS.

Workaround: None. CSCuc73632

- The following (information-only) error message and traceback may occur during MFIB-to-platform state updates for Bidirectional PIM (*,G/m) entries associated with Bidirectional PIM rendezvous points:

```
%SYS-2-NOBLOCK: may_suspend with blocking disabled. -Process= "MFIB_mrib_read", ipl=
0, pid= 370
-Traceback= 1#f95b67f80cdf0886bbf15560d7553abc :152CC000+2699F4C :152CC000+269A310
:152CC000+1F1B55C :152CC000+38D5F4C :152CC000+2C25698 :152CC000+2C2EDF4
:152CC000+5F6F0B0 :152CC000+5F6F1A0 :152CC000+2C2F274 :152CC000+2C24AA4
:152CC000+119935C :152CC000+1D94244 :152CC000+119B070 :152CC000+119699C
:152CC000+2C50D00 :152CC000+2B5901C
```

These messages are typically observed during SSO, bootup, or when a PIM-enabled interface undergoes a state transition on a switch containing Bidir PIM state entries.

Workaround: None. CSCud39208

- Configuring an interface as unidirectional with the **unidirectional send-only | receive-only** command still allows an interface to send (configured as Send-only Unidirection Ethernet mode) or receive (configured as Receive-only Unidirection Ethernet mode) packets in a bidirectional mode.

Workaround: None. CSCui10480

- Following a switchover on VSS, CPU may remain high. The **show platform cpu packet statistics** command displays high usage due to “SA Miss.”

Workaround: Clear the MAC table. CSCuh50329

- Frequent polling of CPU-PROCESS-MIB may cause a switch to unexpectedly reload.

Workaround: None. CSCug65204

- SNMP may time out and produce CPUHOG messages when lldpXMedMIB is polled.

Workaround: CSCuh88726

- A port configured for webauth is not programmed with the default or fallback ACL when sessions enter the INIT state.

Workaround: None. CSCuj71597

- When a device authenticates with dot1x after authenticating with MAB, any policies applied by MAB remain in place.

Workarounds:

- Ensure that the dot1x supplicant always authenticates before MAB.
- Create MAB policies for dot1x hosts that do not supply a URL redirect. CSCui79988

- On a Catalyst 4500 VSS using IOS Release XE 3.4.0SG to 3.4.2SG, or 3.5.0E, the **show platform** command may be truncated with a "Timed out" message and may rarely produce an unexpected reload. The likelihood of a reload increases if the command is issued over an SSH session or if the output is redirected to a file. The same behavior is observed using IOS Release XE 3.5.0 and the **show tech** command.

Workaround: None. CSCul00025

Resolved Caveats for Cisco IOS XE Release 3.4.2SG

This section lists the resolved caveats for Cisco IOS XE Release 3.4.2SG:

- A GLC-GE-100FX pluggable may not operate when used in WS-X4624-SFP-E, WS-X4640-CSFP-E or WS-X4612-SFP-E modules.
Workaround: None CSCui23911
- The switch may reload unexpectedly or become inaccessible when the integrated web server is used, either through direct web access to the switch, or indirectly through the webauth feature.
Workaround: Enter either the **no ip http server** or the **no ip http secure-server** command. This disables the http/s server. CSCui14525

Open Caveats for Cisco IOS XE Release 3.4.1SG

This section lists the open caveats for Cisco IOS XE Release 3.4.1SG:

- When an SNMP query includes the cpmCPUProcessHistoryTable, the query time is very slow, and CPU utilization of the os_info_p process (OS Information provider) increases substantially. The query time of an almost fully populated table is 68 minutes.
Workaround: None. CSCth42248
- The **show ipv6 access-list** command displays incorrect match counts when multicast traffic is matched to an IPv6 access list that is attached to an SVI.
Workaround: None. CSCth65129
- When you configure open authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new Standby supervisor engine. This behavior interrupts traffic only after the second switchover because the new Standby supervisor engine possesses the wrong state after the initial switchover and the second switchover starts the port in the blocking state.
Workaround: Enter **shut** and **no shut** on the port to synchronize the STP state. CSCtf52437
- If you reboot a switch, the configured value of the interface MTU size for the elements of the port channel interface does not work for IPv6 traffic.
Workaround: After the switch reloads, enter **shut** and **no shut** on the port-channel interface. CSCto27085
- Dynamic buffer limiting might not function at queue limits less than or equal to 128.
Workaround: Increase the queue limit to at least 256. CSCto57602
- A device in a guest VLAN that is connected behind a phone capable of 2nd-port-notification experiences packet loss following a SSO failover. The device experiences an authentication restart after the first CDP frame arrives from the phone.
Workaround: None. CSCto46018
- If you perform an OIR on a line card, several %C4K_RKNOVA-4-INVALIDTOKENEXPIRED messages appear in the logs.
Workaround: None. CSCtu37959
- When you enable both Cisco TrustSec and RADIUS accounting, a disparity occurs between the RADIUS client (Cisco switch) and the RADIUS/CTS server in how the authenticator field in the header is computed for DOT1X/RADIUS accounting messages.

A Cisco IOS AAA client uses the PAC secret to compute the authenticator; Cisco Secure ACS 5.2 uses the shared secret. This behavior causes a mismatch that results in a rejection of the accounting message, and the client marks the server as unresponsive.

Workaround: None. You must disable 802.1X accounting. CSCts26844

- When more than one Equal Cost Multipath (ECMP) is available on the downstream switch, and Mediatrace is invoked to provide flow statistics, the dynamic policy does not show statistics for a flow.

Mediatrace cannot find the correct inbound interface and applies the dynamic policy on a different interface from the one used for media flow.

Workaround: None. CSCts20229

- When a switchover is created on the Mediatrace responder, the dynamic access list created for a monitored flow tuple is not deleted. Although the Mediatrace initiator creates another set of dynamic access lists after the switchover, the old ones remain in the configuration.

Stale dynamic access lists force the system to monitor unwanted traffic.

Workarounds:

- If the switchover is scheduled, remove the scheduled session on the initiator and reschedule the session after the new active supervisor engine boots on the responder.
- If the Mediatrace responder SSO is not planned, after the new active supervisor engine boots, manually delete the stale dynamic access lists. CSCty75070

- When you add a "bfd" suffix to the **snmp server host** *x.x.x.x* configuration command, the BFD traps, `ciscoBfdSessUp` and `ciscoBfdSessDown`, are not generated.

Workaround: Do not specify a "bfd" suffix with the **snmp-server host** *x.x.x.x* configuration command. CSCtx51561

- During either a system- or user-initiated reload operation, the following message is observed when the system shuts down:

```
HARDWARE WATCHDOG
```

This message is not observed during a system bootup.

Workaround: None required. This message is information only. CSCtz15738

- In a multichassis port channel on a VSS system with a very high number of link up and down events that occur within a second and typically causes an error-disable event, only the ports on the active switch are error-disabled due to flaps.

Workaround: None. CSCuc36612

- If you enter the **show spi-fc 12** command, a crash occurs.

Workaround: Use the **show spi-fc all** command to dump all SPI channel information. CSCuc81286

- When you enter the **ip pim register-rate-limit** command, the following error message displays:

```
'Failed to configure service policy on register tunnel' and 'STANDBY:Failed to
configure service policy on register tunnel'.
```

Workaround: None. The **ip pim register-rate-limit** command does not function. CSCub32679

- Packets that are routed on the same Layer 3 interface (or SVI) that entered on are dropped if received on the VSS standby switch.

Workaround: None. CSCuj67614

- Ports occasionally stay down after an OIR of a standby line card in VSS.

Workaround: Enter **shut**, then **no shut** to bring up the links. CSCuc37676

- You can attach an input QoS policy to VSL member ports, but you cannot detach it. You only can configure VSL ports.

Workaround: Default the VSL member ports and detach the input QoS policy. CSCuc49150

- When VSS receives a VTP message with information about the creation of 4000 VLANs, traceback and syslog messages (containing EM-4-SEARCH) are displayed.

Workaround: None. You might try reducing the number of VLANs created at one time.

CSCuc66206

- For packets with the same ingress and egress Layer 3 interface, ingress QoS marking policy does not work.

Workaround: Turn off ICMP redirect through the **ip redirect** command. CSCua71929

- On systems performing multicast routing, a brief increase in CPU consumption occurs every few minutes. In large-scale environments, this CPU increase is more noticeable.

Workaround: None. CSCub44553

- When the Wireshark feature is applied on a control panel, it fails to capture the correct packets as they travel to the CPU in VSS, under the following conditions:

- Incoming packets on the VSS standby port are directed to the CPU for host learning.
- Layer 3 exceptions occur for packets arriving on the VSS standby port.
- ACL logging occurs on the VSS standby port.

Workaround: None. CSCub33727

- The POST results on the VSS standby switch displayed by the **show diagnostic result module all detail** command indicate module number 1 rather than 11. The module number is not interpreted by Cisco IOS.

Workaround: None. CSCuc73632

- The following (information-only) error message and traceback may occur during MFIB-to-platform state updates for Bidirectional PIM (*,G/m) entries associated with Bidirectional PIM rendezvous points:

```
%SYS-2-NOBLOCK: may_suspend with blocking disabled. -Process= "MFIB_mrib_read", ipl=
0, pid= 370
-Traceback= 1#f95b67f80cdf0886bbf15560d7553abc :152CC000+2699F4C :152CC000+269A310
:152CC000+1F1B55C :152CC000+38D5F4C :152CC000+2C25698 :152CC000+2C2EDF4
:152CC000+5F6F0B0 :152CC000+5F6F1A0 :152CC000+2C2F274 :152CC000+2C24AA4
:152CC000+119935C :152CC000+1D94244 :152CC000+119B070 :152CC000+119699C
:152CC000+2C50D00 :152CC000+2B5901C
```

These messages are typically observed during SSO, bootup, or when a PIM-enabled interface undergoes a state transition on a switch containing Bidir PIM state entries.

Workaround: None. CSCud39208

- Configuring an interface as unidirectional with the **unidirectional send-only | receive-only** command still allows an interface to send (configured as Send-only Unidirection Ethernet mode) or receive (configured as Receive-only Unidirection Ethernet mode) packets in a bidirectional mode.

Workaround: None. CSCui10480

- The switch may reload unexpectedly or become inaccessible when the integrated web server is used, either through direct web access to the switch, or indirectly through the webauth feature.

- Workaround:** Enter either the **no ip http server** or the **no ip http secure-server** command. This disables the http/s server. CSCui14525
- A GLC-GE-100FX pluggable may not operate when used in WS-X4624-SFP-E, WS-X4640-CSFP-E or WS-X4612-SFP-E modules.

Workaround: None CSCui23911
- Following a switchover on VSS, CPU may remain high. The **show platform cpu packet statistics** command displays high usage due to “SA Miss.”

Workaround: Clear the MAC table. CSCuh50329
- Frequent polling of CPU-PROCESS-MIB may cause a switch to unexpectedly reload.

Workaround: None.CSCug65204
- SNMP may time out and produce CPUHOG messages when lldpXMedMIB is polled.

Workaround: CSCuh88726
- A port configured for webauth is not programmed with the default or fallback ACL when sessions enter the INIT state.

Workaround: None. CSCuj71597
- When a device authenticates with dot1x after authenticating with MAB, any policies applied by MAB remain in place.

Wokarounds:

 - Ensure that the dot1x supplicant always authenticates before MAB.
 - Create MAB policies for dot1x hosts that do not supply a URL redirect. CSCui79988
- On a Catalyst 4500 VSS using IOS Release XE 3.4.0SG to 3.4.2SG, or 3.5.0E, the **show platform** command may be truncated with a "Timed out" message and may rarely produce an unexpected reload. The likelihood of a reload increases if the command is issued over an SSH session or if the output is redirected to a file. The same behavior is observed using IOS Release XE 3.5.0 and the **show tech** command.

Workaround: None. CSCul00025

Resolved Caveats for Cisco IOS XE Release 3.4.1SG

This section lists the resolved caveats for Cisco IOS XE Release 3.4.1SG:

- With IGMP snooping enabled, multicast traffic received through a tunnel interface is not forwarded through the Outgoing Interface List.

Workaround: Disable IGMP snooping. CSCuc65538
- When MLD snooping is enabled, control-plane policing on IPv6 ND packets stops working. This does not impact other control packets.

Workaround: None. CSCua89658
- When a port connected to a CDP, DHCP, or LLDP speaker goes down, a small memory leak occurs (typically less than 300 bytes).

Workaround: Disable these protocols on interfaces that might flap frequently. CSCub85948

- VSS allows you to configure the router MAC address that is used by spanning tree to calculate its bridge ID. When a switchover occurs, this MAC address is retained at the newly active switch. However, the spanning tree bridge ID changes because it uses the local chassis MAC address, instead of the configured router MAC address, to calculate the bridge ID.

Workaround: Ensure that the spanning-tree root is configured in the network. This avoids a topology change. CSCud94151.

- The **show inventory** command does not display mux buffers information on the local chassis after a switchover although this information is displayed prior to a switchover.

Workaround: Enter the **show idprom muxbuffer** command to display the missing information. CSCuc79728

- When the VSS active switch is running and the VSS standby switch is booting, ports on the standby switch boot long before the control plane is fully functional. This may cause channel ports on the standby switch to start working in independent mode before the channel ports are bundled.

Workaround: Do not configure LACP independent mode. Because the PAgP does not have a workaround, it may cause a traffic loss of several seconds until the ports are bundled. This situation occurs only when a switch is booting; it does not apply to a port going down and coming up after bootup. CSCud94258.

- If REP is configured on a dot1q trunk and the native VLAN is administratively set to something other than the default, REP packets are not sent on the native VLAN

Workaround: Retain the trunk native VLAN as 1. CSCud05521

- When a session is neither authenticated nor granted fallback authorization (e.g. by entering **guest-vlan** or **auth-fail-vlan**) in multi-auth mode, unauthenticated sessions remain indefinitely and are not cleared by the system.

Workaround: Clear sessions manually with the **clear authentication sessions** command. CSCtg15739

- **redirect-url** and **redirect-acl** are not cleared after a successful CoA, causing the final step of Central Web Authentication to fail.

Workaround: Return a dACL in the authorization profile with successful guest authentication. CSCue62019

- If URL redirect installed as part of authorization and either of the following occurs, memory will be leaked:

- a fast stream of traffic matches the URL redirect ACL as IPDT clears an address,
- a traffic stream matches the URL redirect ACL and no URL redirect policy is installed for that IP address,

If this occurs repeatedly, IPDT and other control packet processing ultimately ceases.

Workaround: If this behavior completely fills the CPU buffer, the switch must be reloaded. However, the frequency of encountering a stuck queue can be reduced to nearly zero by modifying the URL redirect ACL to permit only 80/443 traffic. CSCug56646

- If a dACL name is too long (about 24 characters, depending on the interface where it is applied), the ACL will be incorrectly shared over multiple ports.

Workaround: Shorten the dACL name. CSCug78653

- On a switches polled for OIDs under CISCO-PROCESS-MIB and running IOS Release XE 3.3.0SG, 3.3.1SG, 3.3.2SG or 3.4.0SG, the **show process memory sorted** command displays an increasing memory usage by the eicored process.

Workaround: Exclude polling of the CISCO-PROCESS-MIB using an SNMP view:

```
snmp-server view restrict iso included
snmp-server view restrict ciscoProcessMIB excluded
snmp-server community cisco view restrict RO
```

CSCud55965

- Whenever a S,G entry expires, a switch shows increasing memory utilization in by the MFIB_mrrib/read/write process.

Workaround: Minimize leak by avoiding S,G deletion events:

- Extend the receiver-less S,G duration (e.g. ip pim sparse sg-expiry-timer <big value>).
- If sources are varied, try to minimize them.
- If some static sources send infrequently, extend the expiry timer to cover the gaps in the packet stream.
- If some receivers are unreliable, consider static joins.

S,G clears:

- Minimize Layer 2 or Layer 3 topology changes that would require multicast reconvergence.
- Avoid manually clearing mroutes. CSCua62262

- A switch running IOS Release XE 3.4.0SG loses all Layer 3 connectivity to or from the switch IP address. Switching is unaffected, but routed IP traffic (snmp, ntp, telnet, ssh, etc.) is affected.

Workaround: Once the problem occurs, reboot the switch.

Disabling Fa1 prevents the problem. CSCue76243

- A switch running IOS Release 3.3.0SG, 3.3.1SG, 3.3.2SG or 3.4.0SG drops some fragmented packets that are routed through the switch. Bridged traffic is unaffected.

Workaround: None. CSCue96534

- SNMPGET queries for CISCO-PROCESS-MIB fail with the message "No Such Instance currently exists at this OID."

Workaround: Use SNMPWALK. CSCtz67068

- If a switch issues CLI commands at a high rate (usually by script), it crashes with a message like the following:

```
%IOSXE-2-PLATFORM: process ng_dumper: Process eicored: terminated abnormally.
```

Workaround: Avoid scripted CLI. CSCtz19897

- On Supervisor Engine 7L-E, MAC address learning does not occur on dot1q-tunnel ports. This behavior is not observed on Supervisor Engine 7-E.

Workaround: None. CSCub01918

Open Caveats for Cisco IOS XE Release 3.4.0SG

This section lists the open caveats for Cisco IOS XE Release 3.4.0SG:

- When an SNMP query includes the cpmCPUProcessHistoryTable, the query time is very slow, and CPU utilization of the os_info_p process (OS Information provider) increases substantially. The query time of an almost fully populated table is 68 minutes.

Workaround: None. CSCth42248

- The **show ipv6 access-list** command displays incorrect match counts when multicast traffic is matched to an IPv6 access list that is attached to an SVI.
Workaround: None. CSCth65129
- When you configure open authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new Standby supervisor engine. This behavior interrupts traffic only after the second switchover because the new Standby supervisor engine possesses the wrong state after the initial switchover and the second switchover starts the port in the blocking state.
Workaround: Enter **shut** and **no shut** on the port to synchronize the STP state. CSCtf52437
- If you reboot a switch, the configured value of the interface MTU size for the elements of the port channel interface does not work for IPv6 traffic.
Workaround: After the switch reloads, enter **shut** and **no shut** on the port-channel interface. CSCto27085
- Dynamic buffer limiting might not function at queue limits less than or equal to 128.
Workaround: Increase the queue limit to at least 256. CSCto57602
- A device in a guest VLAN that is connected behind a phone capable of 2nd-port-notification experiences packet loss following a SSO failover. The device experiences an authentication restart after the first CDP frame arrives from the phone.
Workaround: None. CSCto46018
- If you perform an OIR on a line card, several %C4K_RKNOVA-4-INVALIDTOKENEXPIRED messages appear in the logs.
Workaround: None. CSCtu37959
- When you enable both Cisco TrustSec and RADIUS accounting, a disparity occurs between the RADIUS client (Cisco switch) and the RADIUS/CTS server in how the authenticator field in the header is computed for DOT1X/RADIUS accounting messages.
A Cisco IOS AAA client uses the PAC secret to compute the authenticator; Cisco Secure ACS 5.2 uses the shared secret. This behavior causes a mismatch that results in a rejection of the accounting message, and the client marks the server as unresponsive.
Workaround: None. You must disable 802.1X accounting. CSCts26844
- When more than one Equal Cost Multipath (ECMP) is available on the downstream switch, and Mediatrace is invoked to provide flow statistics, the dynamic policy does not show statistics for a flow.
Mediatrace cannot find the correct inbound interface and applies the dynamic policy on a different interface from the one used for media flow.
Workaround: None. CSCts20229
- When a switchover is created on the Mediatrace responder, the dynamic access list created for a monitored flow tuple is not deleted. Although the Mediatrace initiator creates another set of dynamic access lists after the switchover, the old ones remain in the configuration.
Stale dynamic access lists force the system to monitor unwanted traffic.
Workarounds:
 - If the switchover is scheduled, remove the scheduled session on the initiator and reschedule the session after the new active supervisor engine boots on the responder.
 - If the Mediatrace responder SSO is not planned, after the new active supervisor engine boots, manually delete the stale dynamic access lists. CSCty75070

- Configuring an interface as unidirectional with the **unidirectional send-only | receive-only** command still allows an interface to send (configured as Send-only Unidirection Ethernet mode) or receive (configured as Receive-only Unidirection Ethernet mode) packets in a bidirectional mode.

Workaround: None. CSCui10480

- When you add a "bfd" suffix to the **snmp server host x.x.x.x** configuration command, the BFD traps, ciscoBfdSessUp and ciscoBfdSessDown, are not generated.

Workaround: Do not specify a "bfd" suffix with the **snmp-server host x.x.x.x** configuration command. CSCtx51561

- During either a system- or user-initiated reload operation, the following message is observed when the system shuts down:

```
HARDWARE WATCHDOG
```

This message is not observed during a system bootup.

Workaround: None required. This message is information only. CSCtz15738

- In a multichassis port channel on a VSS system with a very high number of link up and down events that occur within a second and typically causes an error-disable event, only the ports on the active switch are error-disabled due to flaps.

Workaround: None. CSCuc36612

- If you enter the **show spi-fc 12** command, a crash occurs.

Workaround: Use the **show spi-fc all** command to dump all SPI channel information. CSCuc81286

- When you enter the **ip pim register-rate-limit** command, the following error message displays:

```
'Failed to configure service policy on register tunnel' and 'STANDBY:Failed to
configure service policy on register tunnel'.
```

Workaround: None. The **ip pim register-rate-limit** command does not function. CSCub32679

- Packets that are routed on the same Layer 3 interface (or SVI) that entered on are dropped if received on the VSS standby switch.

Workaround: None. CSCuj67614

- Ports occasionally stay down after an OIR of a standby line card in VSS.

Workaround: Enter **shut**, then **no shut** to bring up the links. CSCuc37676

- You can attach an input QoS policy to VSL member ports, but you cannot detach it. You only can configure VSL ports.

Workaround: Default the VSL member ports and detach the input QoS policy. CSCuc49150

- With IGMP snooping enabled, multicast traffic received through a tunnel interface is not forwarded through the Outgoing Interface List.

Workaround: Disable IGMP snooping. CSCuc65538

- When VSS receives a VTP message with information about the creation of 4000 VLANs, traceback and syslog messages (containing EM-4-SEARCH) are displayed.

Workaround: None. You might try reducing the number of VLANs created at one time.
CSCuc66206

- For packets with the same ingress and egress Layer 3 interface, ingress QoS marking policy does not work.

Workaround: Turn off ICMP redirect through the **ip redirect** command. CSCua71929

- On systems performing multicast routing, a brief increase in CPU consumption occurs every few minutes. In large-scale environments, this CPU increase is more noticeable.

Workaround: None. CSCub44553

- When the Wireshark feature is applied on a control panel, it fails to capture the correct packets as they travel to the CPU in VSS, under the following conditions:
 - Incoming packets on the VSS standby port are directed to the CPU for host learning.
 - Layer 3 exceptions occur for packets arriving on the VSS standby port.
 - ACL logging occurs on the VSS standby port.

Workaround: None. CSCub33727

- The POST results on the VSS standby switch displayed by the **show diagnostic result module all detail** command indicate module number 1 rather than 11. The module number is not interpreted by Cisco IOS.

Workaround: None. CSCuc73632

- The **show inventory** command does not display mux buffers information on the local chassis after a switchover although this information is displayed prior to a switchover.

Workaround: Enter the **show idprom muxbuffer** command to display the missing information. CSCuc79728

- The following (information-only) error message and traceback may occur during MFIB-to-platform state updates for Bidirectional PIM (*,G/m) entries associated with Bidirectional PIM rendezvous points:

```
%SYS-2-NOBLOCK: may_suspend with blocking disabled. -Process= "MFIB_mrib_read", ipl=
0, pid= 370
-Traceback= 1#f95b67f80cdf0886bbf15560d7553abc :152CC000+2699F4C :152CC000+269A310
:152CC000+1F1B55C :152CC000+38D5F4C :152CC000+2C25698 :152CC000+2C2EDF4
:152CC000+5F6F0B0 :152CC000+5F6F1A0 :152CC000+2C2F274 :152CC000+2C24AA4
:152CC000+119935C :152CC000+1D94244 :152CC000+119B070 :152CC000+119699C
:152CC000+2C50D00 :152CC000+2B5901C
```

These messages are typically observed during SSO, bootup, or when a PIM-enabled interface undergoes a state transition on a switch containing Bidir PIM state entries.

Workaround: None. CSCud39208

- When a port connected to a CDP, DHCP, or LLDP speaker goes down, a small memory leak occurs (typically less than 300 bytes).

Workaround: Disable these protocols on interfaces that might flap frequently. CSCub85948

- VSS allows you to configure the router MAC address that is used by spanning tree to calculate its bridge ID. When a switchover occurs, this MAC address is retained at the newly active switch. However, the spanning tree bridge ID changes because it uses the local chassis MAC address, instead of the configured router MAC address, to calculate the bridge ID.

Workaround: Ensure that the spanning-tree root is configured in the network. This avoids a topology change. CSCud94151.

- When the VSS active switch is running and the VSS standby switch is booting, ports on the standby switch boot long before the control plane is fully functional. This may cause channel ports on the standby switch to start working in independent mode before the channel ports are bundled.

Workaround: Do not configure LACP independent mode. Because the PAgP does not have a workaround, it may cause a traffic loss of several seconds until the ports are bundled. This situation occurs only when a switch is booting; it does not apply to a port going down and coming up after bootup. CSCud94258.

- When a port connected to a CDP, DHCP, or LLDP speaker goes down, a small memory leak occurs (typically less than 300 bytes).

Workaround: Disable these protocols on interfaces that might flap frequently. CSCub85948

- When MLD snooping is enabled, control-plane policing on IPv6 ND packets stops working. This does not impact other control packets.

Workaround: None. CSCua89658

- If REP is configured on a dot1q trunk and the native VLAN is administratively set to something other than the default, REP packets are not sent on the native VLAN

Workaround: Retain the trunk native VLAN as 1. CSCud05521

- When a session is neither authenticated nor granted fallback authorization (e.g. by entering **guest-vlan** or **auth-fail-vlan**) in multi-auth mode, unauthenticated sessions remain indefinitely and are not cleared by the system.

Workaround: Clear sessions manually with the **clear authentication sessions** command. CSCtg15739

- `redirect-url` and `redirect-acl` are not cleared after a successful CoA, causing the final step of Central Web Authentication to fail.

Workaround: Return a dACL in the authorization profile with successful guest authentication. CSCue62019

- If URL redirect installed as part of authorization and either of the following occurs, memory will be leaked:
 - a fast stream of traffic matches the URL redirect ACL as IPDT clears an address,
 - a traffic stream matches the URL redirect ACL and no URL redirect policy is installed for that IP address,

If this occurs repeatedly, IPDT and other control packet processing ultimately ceases.

Workaround: If this behavior completely fills the CPU buffer, the switch must be reloaded. However, the frequency of encountering a stuck queue can be reduced to nearly zero by modifying the URL redirect ACL to permit only 80/443 traffic. CSCug56646

- If a dACL name is too long (about 24 characters, depending on the interface where it is applied), the ACL will be incorrectly shared over multiple ports.

Workaround: Shorten the dACL name. CSCug78653

- On a switches polled for OIDs under CISCO-PROCESS-MIB and running IOS Release XE 3.3.0SG, 3.3.1SG, 3.3.2SG or 3.4.0SG, the **show process memory sorted** command displays an increasing memory usage by the eicored process.

Workaround: Exclude polling of the CISCO-PROCESS-MIB using an SNMP view:

```
snmp-server view restrict iso included
snmp-server view restrict ciscoProcessMIB excluded
snmp-server community cisco view restrict RO
```

CSCud55965

- Whenever a S,G entry expires, a switch shows increasing memory utilization in by the MFIB_mrrib/read/write process.
Workaround: Minimize leak by avoiding S,G deletion events:
 - Extend the receiver-less S,G duration (e.g. ip pim sparse sg-expiry-timer <big value>).
 - If sources are varied, try to minimize them.
 - If some static sources send infrequently, extend the expiry timer to cover the gaps in the packet stream.
 - If some receivers are unreliable, consider static joins.
 S,G clears:
 - Minimize Layer 2 or Layer 3 topology changes that would require multicast reconvergence.
 - Avoid manually clearing mroutes. CSCua62262
- A switch running IOS Release XE 3.4.0SG loses all Layer 3 connectivity to or from the switch IP address. Switching is unaffected, but routed IP traffic (snmp, ntp, telnet, ssh, etc.) is affected.
Workaround: Once the problem occurs, reboot the switch.
 Disabling Fa1 prevents the problem. CSCue76243
- A switch running IOS Release 15.1(1)SG, 15.1(1)SG1, 15.1(1)SG2, or 15.1(2)SG, drops some fragmented packets that are routed through the switch. Bridged traffic is unaffected.
Workaround: None. CSCue96534
- SNMPGET queries for CISCO-PROCESS-MIB fail with the message "No Such Instance currently exists at this OID."
Workaround: Use SNMPWALK. CSCtz67068
- If a switch issues CLI commands at a high rate (usually by script), it crashes with a message like the following:

```
%IOSXE-2-PLATFORM: process ng_dumper: Process eicored: terminated abnormally.
```

Workaround: Avoid scripted CLI. CSCtz19897
- On Supervisor Engine 7L-E, MAC address learning does not occur on dot1q-tunnel ports.
 This behavior is not observed on Supervisor Engine 7-E.
Workaround: None. CSCub01918
- From Cisco IOS Release XE 3.2.0 onwards, configuring an interface as uni-directional with the **unidirectional send-only | receive-only** command, still allows the interface to send or receive packets in a bi-directional mode. An interface that is configured as "Send-only Unidirection Ethernet mode" receives the packets; an interface configured as "Receive-only Unidirection Ethernet mode" sends the packets.
Workaround: None. CSCui10480
- A GLC-GE-100FX pluggable may not operate when used in WS-X4624-SFP-E, WS-X4640-CSFP-E or WS-X4612-SFP-E modules.
Workaround: None CSCui23911
- Following a switchover on VSS, CPU may remain high. The **show platform cpu packet statistics** command displays high usage due to "SA Miss."
Workaround: Clear the MAC table. CSCuh50329
- Frequent polling of CPU-PROCESS-MIB may cause a switch to unexpectedly reload.

Workaround: None. CSCug65204

- SNMP may time out and produce CPUHOG messages when lldpXMedMIB is polled.

Workaround: CSCuh88726

- On a Catalyst 4500 VSS using IOS Release XE 3.4.0SG to 3.4.2SG, or 3.5.0E, the **show platform** command may be truncated with a "Timed out" message and may rarely produce an unexpected reload. The likelihood of a reload increases if the command is issued over an SSH session or if the output is redirected to a file. The same behavior is observed using IOS Release XE 3.5.0 and the **show tech** command.

Workaround: None. CSCul00025

Resolved Caveats for Cisco IOS XE Release 3.4.0SG

This section lists the resolved caveats for Cisco IOS XE Release 3.4.0SG:

- Following an upgrade to IOS Release XE 3.3.1SG, the following error messages might display for switches with PWR-C45-4200ACV power supplies:

```
%C4K_CHASSIS-3-INSUFFICIENTPOWERSUPPLIESDETECTED: Insufficient power supplies present
for specified config
```

```
%C4K_CHASSIS-3-MIXINVOLTAGEDETECTED: Power supplies in the chassis are receiving
different voltage inputs
```

```
%C4K_CHASSIS-3-MIXINPOWERDETECTED: Power supplies in the chassis are of different
types (AC/DC) or wattage
```

Use the **show power** command to determine whether 220V inputs are incorrectly detected as “off” or 110V.

Workaround: Unseat or reseat the impacted power supply and turn on the input power. CSCuc50555.

- Dynamic ACLs do not function correctly if they have advanced operators, including dscp/ipp/tos, log/log-input, fragments, and TCP flag operators.

Workaround: Remove these operators from any dynamic ACLs. CSCts05302

- A peer policy is not updated after reauthentication if the policy is changed on the AS beforehand. After reauthentication, the original peer policy is retained.

Workaround: Enter **shut** and **no shut** on the port. CSCts29515

- A switch running a Supervisor Engine 7-E or Supervisor Engine 7L-E fails if you enter **show memory debug leak** on the console while **show memory detailed process iosd debug leaks** is being executed from another Telnet session.

Workaround: Avoid running both commands simultaneously. CSCty27680

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>

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:

- Catalyst 4500E release notes are available at:
http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_release_notes_list.html

Software documents for the Catalyst 4500 Classic, Catalyst 4500 E-Series, Catalyst 4900 Series, and Catalyst 4500-X Series switches are available at the following URLs:

- *Catalyst 4500 Series Software Configuration Guide*
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- *Catalyst 4500 Series Software Command Reference*
http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_command_reference_list.html
- *Catalyst 4500 Series Software System Message Guide*
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_system_message_guides_list.html

Cisco IOS Documentation

Platform-independent Cisco IOS documentation may also apply to the Catalyst 4500 and 4900 switches. These documents are available at the following URLs:

- Cisco IOS configuration guides, Release 12.x

http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html

- Cisco IOS command references, Release 12.x

http://www.cisco.com/en/US/products/ps6350/prod_command_reference_list.html

You can also use the Command Lookup Tool at:

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

- Cisco IOS system messages, version 12.x

http://www.cisco.com/en/US/products/ps6350/products_system_message_guides_list.html

You can also use the Error Message Decoder tool at:

<http://www.cisco.com/pcgi-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.

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

Original SSLeay License:

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

This package is an SSL implementation written by Eric Young (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).

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 acknowledgement:

“This product includes cryptographic software written by Eric Young (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].

Obtaining Documentation and Submitting a Service Request

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

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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)

Release Notes for the Catalyst 4500E Series Switch, Cisco Release IOS XE 3.4.X SG
Copyright © 2013-2015, Cisco Systems, Inc. All rights reserved.

