Release Notes for the Catalyst 4500E Series Switch, Cisco IOS XE Release 3.5.xE

Current release
IOS XE 3.5.3E—July 7, 2014

Prior release
IOS XE 3.5.2E, IOS XE 3.5.1E, IOS XE 3.5.0E—August 26, 2013

This release note describes the features, modifications, and caveats for the Cisco IOS XE 3.5.0E software on the Catalyst 4500E series switch with Supervisor Engine 7-E and 7L-E.

Cisco IOS Software Release XE 3.5.0E is part of the new software releases on Cisco Catalyst 2960S, 2960C, 3560C, 3750-X, 3560-X, 4500E and 4500-X, 4900M, and 4948E/E-F Series Switches. These releases deliver new software and hardware innovations in campus access and aggregation deployments that span across many technologies, including enhanced support for IPv6, security, high availability, and IP multicast.

Support for Cisco IOS XE Release 3.5.0E 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

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

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

The LAN Base image complements the existing IP Base and Enterprise Services images. It is focused on customer access and Layer 2 requirements and therefore many of the IP Base features are not required. The IP upgrade image is available if at a later date you require some of those features

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

Cisco XE Release Strategy

Customers with Catalyst 4500 Series Switches who need the latest hardware and software features should migrate to Cisco IOS Release XE 3.5.0E.

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.

IOS XE 3.2.xSG is the recommended release for customers who require a release with a maintenance train

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*
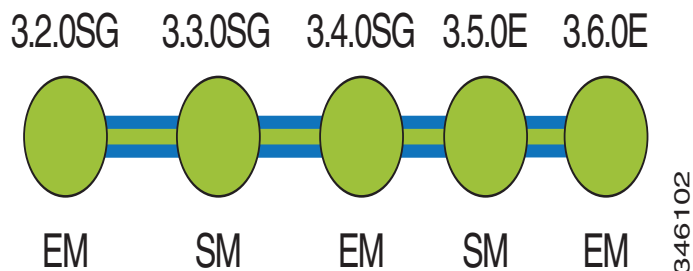
Support

Support for Cisco IOS Software Release XE 3.5.0E 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

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

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

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-LX	48-port 1000BASE-LX (small form-factor pluggable) Gigabit Ethernet fiber optic interface switching module
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)
WS-X4648-RJ45-E	48 port 10/100/1000BT with 2 to 1 oversubscription and jumbo frame support
WS-X4648-RJ45V-E	48 port 10/100/1000 Mb with 2 to 1 oversubscription PoE 802.3af providing up to 20 Watts power/port
WS-X4648-RJ45V+E	48 port 10/100/1000 Mb with 2 to 1 oversubscription PoE 802.3at providing up to 30 Watts power/port
WS-X4748-RJ45V+E	48-port 10/100/1000 line card nonblocking PoE 802.3at providing up to 30 Watts power/port
WS-X4748-UPOE+E	48-port 10/100/1000 line card nonblocking PoE 802.3at and 60 watt UPOE PoE linecard with Ethernet Energy Efficient feature.
WS-X4748-RJ45-E	48-port 10/100/1000 nonblocking line card with the Ethernet Energy Efficient feature
WS-X4748-SFP-E	48-port 1000Base-X SFP (small form factor pluggable) line card
WS-X4724-SFP-E	24-port 1000Base-X SFP (small form factor pluggable) line card
WS-X4712-SFP-E	12-port 1000Base-X SFP (small form factor pluggable) line card
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

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-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
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
Small Form-Factor Pluggable Gigabit Ethernet Modules	
GLC-BX-D	1000BASE-BX10-D small form-factor pluggable module
GLC-BX-U	1000BASE-BX10-U small form-factor pluggable module
GLC-EX-SMD	1000BASE-EX GE SFP ports
GLC-SX-MM	1000BASE-SX small form-factor pluggable module
GLC-SX-MMD	1000BASE-SX small form-factor pluggable module with DOM support
GLC-LH-SM	1000BASE-LX/LH small form-factor pluggable module
GLC-LH-SMD	1000BASE-LX/LH small form-factor pluggable module with DOM support
GLC-ZX-SMD	1000BASE-ZX small form-factor pluggable module with DOM support
GLC-T	1000BASE-T small form-factor pluggable module
CVR-X2-SFP	TwinGig Converter Module; converts a 10 Gigabit Ethernet X2 interface into two Gigabit Ethernet Small Form-Factor Pluggable (SFP) ports.
CWDM-SFP-xxxx	CWDM small form-factor pluggable module (See Table 2 on page 7 for a list of supported wavelengths.)
SFP-DWDM	Dense Wavelength-Division Multiplexing (DWDM) Small Form Factor Pluggable (SFP) module
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

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**
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.
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+-DWDM	10GBASE Dense Wavelength-Division Multiplexing (DWDM) SFP+ 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 7 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

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-C45-2800ACV	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
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, Supervisor Engine 7L-E, and WS-4712-SFP+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

Table 3   *DWDM SFP Supported Wavelengths on Cisco Catalyst 4500E Supervisor Engine 7-E, Supervisor Engine 7L-E, and WS-4712-SFP+E*

Product Number (append with "=" for spares)	**Product Description**
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
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 transceiver module compatibility information, please refer to the URL:

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

Supported E Series Hardware on Cisco IOS XE Release 3.5.0E

A brief list of primary E-Series hardware supported by Cisco IOS XE Release 3.5.0E is shown in Table 4.

Table 4   *Supported E-Series Hardware*

Product Number	Description
WS-C4503-E	Cisco Catalyst 4500E Series 3-Slot Chassis • Fan tray • No Power Supply
WS-C4506-E	Cisco Catalyst 4500E Series 6-Slot Chassis • Fan tray • No Power Supply
WS-C4507R-E	Cisco Catalyst 4500E Series 7-Slot Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 3 and/or 4; the backplane will enforce this restriction.
WS-C4507R+E	Cisco Catalyst 4500E Series 7-Slot 48 GB-ready Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 3 and/or 4; the backplane will enforce this restriction.
WS-C4510R-E	Cisco Catalyst 4500E Series 10-Slot Chassis **Note** This chassis does not support the Supervisor Engine 7L-E. • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 5 and/or 6; the backplane will enforce this restriction.
WS-C4510R+E	Cisco Catalyst 4500E Series 10-Slot 48 GB-ready Chassis **Note** This chassis does not support the Supervisor Engine 7L-E. • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 5 and/or 6; the backplane will enforce this restriction.

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 3.5.0E 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
Cisco Service Discovery Gateway Support	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

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 Change Notification and Logging	No	Yes	Yes
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
Diffserv MIB	Yes	Yes	Yes
DSCP/CoS via LLDP	Yes	Yes	Yes
Duplication Location Reporting Issue	No	Yes	Yes
Dynamic Trunking Protocol (DTP)	Yes	Yes	Yes
Easy Virtual Network (EVN)	No	No	Yes
EIGRP	No	No	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
EIGRP Service Advertisement Framework	Yes	Yes	Yes
EIGRP Stub Routing	No	Yes	Yes
Embedded Event Manager (EEM) 3.2	No	Yes	Yes
Embedded Syslog Manager (ESM)	Yes	Yes	Yes
Energywise Agentless SNMP support	Yes	Yes	Yes
Energywise Wake-On-Lan Support	Yes	Yes	Yes
Enhanced PoE Support (Additional Wattage Range)	Yes	Yes	Yes
Entity API for Physical and Logical Mgd Entities	Yes	Yes	Yes
ErrDisable timeout	Yes	Yes	Yes
EtherChannel	Yes	Yes	Yes
EtherChannel Flexible PAgP	Yes	Yes	Yes
EtherChannel Single Port Channel	Yes	Yes	Yes
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 - Application ID	No	Yes	Yes
Flexible NetFlow - Device type	No	Yes	Yes
Flexible NetFlow - Ethertype	No	Yes	Yes
Flexible NetFlow - Full Flow support	No	Yes	Yes
Flexible NetFlow - Ingress support	No	Yes	Yes
Flexible NetFlow - IPv4 Unicast Flows	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 - IPv6 Unicast Flows	No	Yes	Yes
Flexible NetFlow - Layer 2 Fields	No	Yes	Yes
Flexible NetFlow - Multiple User Defined Caches	No	Yes	Yes
Flexible NetFlow - NetFlow Export over IPv4	No	Yes	Yes
Flexible NetFlow - NetFlowV5 Export protocol	No	Yes	Yes
Flexible NetFlow - NetFlow v9 Export Format	No	Yes	Yes
Flexible NetFlow - Power Reading	No	Yes	Yes
Flexible NetFlow - Username	No	Yes	Yes
Flexible NetFlow - VLAN ID support	No	Yes	Yes
Flexible NetFlow - Export to an IPv6 address	No	Yes	Yes
Flexible NetFlow - IPFIX	No	Yes	Yes
Flex Links+(VLAN Load balancing)	Yes	Yes	Yes
Forced 10/100 Autonegotiation	Yes	Yes	Yes
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

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 802.1s 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
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

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 802.3af PoE (Power over Ethernet)	Yes	Yes	Yes
IEEE 802.3x Flow Control	Yes	Yes	Yes
IGMP Fast Leave	Yes	Yes	Yes
IGMP Filtering	Yes	Yes	Yes
IGMP Snooping	Yes	Yes	Yes
IGMP Version 1	Yes	Yes	Yes
IGMP Version 2	Yes	Yes	Yes
IGMP Version 3	Yes	Yes	Yes
IGMP Version 3 - Explicit Tracking of Hosts, Groups, and Channels	Yes	Yes	Yes
IGMPv3 Host Stack	Yes	Yes	Yes
IGMPv3 Snooping: Full Support	Yes	Yes	Yes
Image Verification	Yes	Yes	Yes
Individual SNMP Trap Support	Yes	Yes	Yes
Inline Power Auto Negotiation	Yes	Yes	Yes
Inline Power Management	Yes	Yes	Yes
Interface Index Persistence	Yes	Yes	Yes
Interface Range Specification	Yes	Yes	Yes
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

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 - DHCP Operations	No	Yes	Yes
IP SLAs - Distribution of Statistics	No	Yes	Yes
IP SLAs - DNS Operation	No	Yes	Yes
IP SLAs - FTP Operation	No	Yes	Yes
IP SLA - HTTP Operation	No	Yes	Yes
IP SLAs - ICMP Echo Operation	No	Yes	Yes
IP SLAs - ICMP Path Echo Operation	No	Yes	Yes
IP SLAs - Multi Operation Scheduler	No	Yes	Yes
IP SLAs - One Way Measurement	No	Yes	Yes
IP SLAs - Path Jitter Operation	No	Yes	Yes
IP SLAs - Random Scheduler	No	Yes	Yes
IP SLAs - Reaction Threshold	No	Yes	Yes
IP SLAs - Responder	Yes	Yes	Yes
IP SLAs - Scheduler	No	Yes	Yes
IP SLAs - Sub-millisecond Accuracy Improvements	No	Yes	Yes
IP SLAs - TCP Connect Operation	No	Yes	Yes
IP SLAs - UDP Based VoIP Operation	No	Yes	Yes
IP SLAs - UDP Echo Operation	No	Yes	Yes
IP SLAs - UDP Jitter Operation	No	Yes	Yes
IP SLAs - Video Operations	No	Yes	Yes
IP SLAs - VoIP Threshold Traps	No	Yes	Yes
IP Summary Address for RIPv2	No	Yes	Yes
IP Unnumbered for VLAN-SVI interfaces	No	Yes	Yes
IPSG (IP Source Guard) v4	Yes	Yes	Yes
IPSG (IP Source Guard) v4 for Static Hosts	Yes	Yes	Yes
IPv4 Policy Based Routing (PBR)	No	No	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
IPv4 Policy-Based Routing (PBR) Recursive Next Hop	No	No	Yes
IPv4 Routing: Static Hosts/Default Gateway	Yes	Yes	Yes
IPv6 / v4 BFD with OSPF/ BGP/ EIGRP and Static	No	Yes	Yes
IPv6 BGP	No	No	Yes
IPv6 Bootstrap Router (BSR) Scoped Zone Support	No	No	Yes
IPv6 CNS Agents	Yes	Yes	Yes
IPv6 Config Logger	Yes	Yes	Yes
IPv6 First Hop Security (FHS): DHCPv6 Guard IPv6 Destination Guard IPv6 Snooping (Data Gleaning, per-limit Address Limit) IPv6 Neighbor Discovery Multicast Suppression IPv6 Router Advertisement (RA) Guard	Yes	Yes	Yes
IPv6 First Hop Security (FHS) Phase 2: Binding table recovery Lightweight DHCPv6 Relay Agent (LDRA) Neighbor Discovery (ND) Multicast Suppress Source and Prefix Guard[2]	Yes	Yes	Yes
IPv6 HSRP	No	Yes	Yes
IPv6 HTTP(S)	Yes	Yes	Yes
IPv6 ICMPv6	Yes	Yes	Yes
IPv6 ICMPv6 Redirect	Yes	Yes	Yes
IPv6 Interface Statistics	Yes	Yes	Yes
IPv6 IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	No	Yes	Yes
IPv6 TCL	Yes	Yes	Yes
IPv6 (Internet Protocol Version 6)	Yes	Yes	Yes
IPv6 Interface Statistics	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 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
IPv6 Multicast: Scope Boundaries	No	Yes	Yes
IPv6 Neighbor Discovery Duplicate Address Detection	Yes	Yes	Yes
IPv6 OSPFv3 NSF/SSO	No	Yes[3]	Yes
IPv6 OSPFv3 Fast Convergence	No	Yes[3]	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[3]	Yes
IPv6 Routing: RIP for IPv6 (RIPng)	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 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
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

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
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
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

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
Multicast HA (NSF/SSO) for IPv4&IPv6	No	Yes	Yes
Multicast Routing Monitor (MRM)	No	No	Yes
Multicast Source Discovery Protocol (MSDP)	No	Yes	Yes
Multicast Subsecond Convergence	No	Yes	Yes
Multicast VLAN Registration (MVR)	Yes	Yes	Yes
NAC - L2 IEEE 802.1x	Yes	Yes	Yes
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
NMSP Enhancements • 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

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
NTP for VRF aware	No	No	Yes
Onboard Failure Logging (OBFL)	Yes	Yes	Yes
OSPF	No	Yes[3]	Yes
OSPF v3 Authentication	No	Yes[3]	Yes
OSPF Flooding Reduction	No	Yes[3]	Yes
OSPF for Routed Access[4]	No	Yes	Yes
OSPF Incremental Shortest Path First (i-SPF) Support	No	Yes[3]	Yes
OSPF Link State Database Overload Protection	No	Yes[3]	Yes
OSPF Not-So-Stubby Areas (NSSA)	No	Yes[3]	Yes
OSPF Packet Pacing	No	Yes[3]	Yes
OSPF Shortest Paths First Throttling	No	Yes[3]	Yes
OSPF Stub Router Advertisement	No	Yes[3]	Yes
OSPF Support for Fast Hellos	No	Yes[3]	Yes
OSPF Support for Link State Advertisement (LSA) Throttling	No	Yes[3]	Yes
OSPF Support for Multi-VRF on CE Routers	No	Yes[3]	Yes
OSPF Update Packet-Pacing Configurable Timers	No	Yes[3]	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

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
PIM Version 2	No	Yes	Yes
PoEP via LLDP	Yes	Yes	Yes
Port Security	Yes (supports 1024 MACs)	Yes (supports 3072 MACs)	Yes (supports 3072 MACs)s
Port Security on Etherchannel Trunk Port	Yes	Yes	Yes
Pragmatic General Multicast (PGM)	No	Yes	Yes
Priority Queueing (PQ)	Yes	Yes	Yes
Private VLAN Promiscuous Trunk Port	Yes	Yes	Yes
Private VLAN Trunk Ports	Yes	Yes	Yes
Private VLANs	Yes	Yes	Yes
Propagation of Location Info over CDP	Yes	Yes	Yes
PVLAN over EtherChannel	Yes	Yes	Yes
PVST + (Per VLAN Spanning Tree Plus)	Yes	Yes	Yes
Q-in-Q	Yes	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

*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
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—Configuration-only Deployment and Smooth Upgrade	Yes	Yes	Yes
Smart Port	Yes	Yes	Yes
SNMP (Simple Network Management Protocol)	Yes	Yes	Yes
SNMP Inform Request	Yes	Yes	Yes
SNMP Manager	Yes	Yes	Yes
SNMPv2C	Yes	Yes	Yes
SNMPv3 - 3DES and AES Encryption Support	Yes	Yes	Yes
SNMPv3 (SNMP Version 3)	Yes	Yes	Yes
Source Specific Multicast (SSM)	No	Yes	Yes
Source Specific Multicast (SSM) - IGMPv3,IGMP v3lite, and URD	No	Yes	Yes
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

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
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
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

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
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)[5]	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
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
TrustSec SGT/ SGA	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

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
Virtual Switching System (VSS)	No	Yes (SUP7E only)	Yes
Virtual Switching System (VSS) Phase 2[6] • Support for Layer 3 MEC—VSS with Layer 3 Multichassis EtherChannel (MEC) at the aggregation layer • Support for VSLP Fast Hello—With VSLP Fast Hello, the Catalyst 4500-X configured for VSS can now connect Access Switches that do not support the ePAgP protocol. • Support for VSL Encryption • Support for Asymmetrix chassis	No	Yes (SUP7E) No (SUP7LE)	Yes (SUP7E) Yes (SUP7LE)
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
VRF-lite for IPv6 on OSPF/ BGP/ EIGRP	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
XML-PI	Yes	Yes	Yes

1. EEE 802.1t—An IEEE amendment to IEEE 802.1D that includes extended system ID, long path cost, and PortFast.

2. When either Source or Prefix Guard for IPv6 is enabled, ICMPv6 packets are unrestricted on all Catalyst 4500 series switch platforms running IOS Cisco Release 15.2(1)E. All other traffic types are restricted.

3. IP Base supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 200 dynamically learned routes.

4. OSPF for Routed Access supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 1000 dynamically learned routes.

5. TDR is not supported on 46xx linecards.

6. VSS supports Smart Install Director—Zero Touch installation without any convergence down-time

MIB Support

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

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

Features Not Supported on the Cisco Catalyst 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 3.5.0E Product Numbers and Images for the Catalyst 4500E Series Switch*

Product Number	Description	Image
S45EU-35-1521E	CAT4500e SUP7-E/SUP7L-E Universal Image	cat4500e-universal.SPA.03.05.00.E.152-1.E.bin
S45EUK9-35-1521E	CAT4500e SUP7-E/SUP7L-E Universal Crypto Image	cat4500e-universalk9.SPA.03.05.00.E.152-1.E.bin
S45EUN-35-1521E	CAT4500e SUP7-E/SUP7L-E Universal No MACSEC Image	cat4500e-universalk9npe.SPA.03.05.00.E.152-1.E.bin

New and Changed Information

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

New Hardware Features in Release IOS XE 3.5.0E

* GLC-T
* SFP+-DWDM
* WS-X4640-CSFP-E on a 10-Slot Catalyst 4500E Chassis

- WS-X4748-SFP-E
- WS-X4724-SFP-E
- WS-X4712-SFP-E

New Software Features in Release IOS XE 3.5.0E

4 byte BGP ASN numbers

BFD v4 and v6

- BFD Infra (VRF-aware; v4 + v6)
- BGP Client for BFD
- OSPFv2 Client for BFD
- EIGRP Client for BFD
- Static Route Client for BFD
- Static Route support for BFD over IPv6

BGP

- malformed attribute error handling
- Cisco-BGP-MIBv2
- Graceful Shutdown
- Add-Path
- VRF dynamic route leaking (for VRF lite)

Binding Integrity Guard (chassis)

Diffserv MIB (RFC 3289) support

Common Criteria

Configurable TCP Keep Alive Timer.

DCM 2.0

DHCP Glean

DHCPv6 Relay Chaining and Route Insertion

Disable IPX in EIGRP

DNS IPv6 Transport for DNS

EIGRP add-path

EIGRP New Release Enablement

- EIGRP IPv6 NSF/GR
- EIGRP MIB
- EIGRP IPv6 MIBs

EIGRP Wide Metrics (Existing)

Enhancement to create global IPv6 entries for unsolicited NA

Enabling v4 PIM in IPBase Package

Encrypt "PMK" password inside the switch (e.g., **show command**)

Energywise Agentless SNMP support

Energywise Wake-On-Lan Support

Flexible Netflow: Application ID

Flexible Netflow: Device Type

Flexible Netflow: Ethertype

Flexible Netflow: Export to an IPv6 address

Flexible Netflow: IPFIX

Flexible Netflow: Power reading

Flexible Netflow: Username

FIPS 140-2

Generate SNMP trap when EIGRP neighbor down

Hop by Hop EH ACL Throttling

HSRP aware PIM

Improved performance for Wireshark

IPv6 Compliance Features (JITC, USGv6)

- Updated ICMP RFCs 4291, 4443, 3484, 2526, 4861, 4862, 5095, 4007, 3513
- UDP MIB (RFC 4113) and TCP MIB (RFC 4022) support
- VRRP over IPv6 (Existing)

IPv6 Duplicate Address Detection (DAD) proxy

IPv6 First Hop Security Phase II

- Binding table recovery
- Bulk Lease Query support from Lightweight DHCPv6 Relay Agent (LDRA)
- Neighbor Discovery (ND) Multicast Suppress
- Prefix Guard
- RA Throttler
- Source Guard

> **Note** When either Source or Prefix Guard for IPv6 is enabled, ICMPv6 packets are unrestricted on all Catalyst 4500 series switch platforms running IOS Cisco Release 15.2(1)E. All other traffic types are restricted.

Ipv6 nd cache expire

IPv6 Neighbor Discovery Multicast Suppress

IPv6 support for TFTP

Layer 3 Multichassis Ethernet Channel

Legacy Line Cards Support in VSS system

- WS-X4148-FX-MT
- WS-X4148-RJ
- WS-X4248-FE-SFP

- WS-X4248-RJ45V

- WS-X4232-L3

- WS-X4306-GB

- WS-X4448-GB-SFP

- WS-X4548-RJ45V+

Manually Configured Tunnel over IPv4

Multicast VLAN Registration (MVR)

Manually Configured Tunnel over IPv4

mDNS Bonjour Support

MIB Gaps

- CISCO-EMBEDDED-EVENT-MGR-MIB

- SNMP-COMMUNITY-MIB

ND Multicast Suppress

Need option to configure exponential backoff for NS timer used in NUD

Netconf XML PI show output

New AutoQoS Show Commands

OSPF feature enablement

- OSPFv2 NSR

- OSPFv3 NSR

- OSPFv3 BFD

- OSPFv3 Graceful Shutdown

- OSPFv2 NSSA

- OSPFv3 NSSA Option

- OSPFv3 External Path Preference

- OSPFv3 Router Max metric Router LSA

- OSPFv3 Retransmission Limit

OSPFv3 Area Filter/DC Ignore

OSPFv3 MIB, OSPF MIB

OSPFv3 Prefix Suppression

Performance Monitor Synchronization

RA Guard

RA Throttler

Route Tag Enhancements

RTU Licensing

Script based zero touch provisioning

SGA (SGT) Deployability Enhancements

- TrustSec Security Group Name Download

- CISCO-TRUSTSEC-POLICY-MIB

- SGA CoA

SGT/SGACL

- Layer 2 SGACL for IPv4 Unicast Traffic
- TrustSec SGACL L2 Bridged Forwarding
- Layer 2 SGT Tagging
- VLAN SGT Mapping

Smart Install Configuration-Only Deployment

SMI Image only upgrade

Smart Install Upgrade Fallback

SMI Director Support with VSS

VRF-aware OSPFv3,EIGRPv6, and BGPv6

- VRF-Lite for OSPFv3
- VRF-Lite for IPv6 EIGRP
- VRF-Lite for BGPv6

VRF aware SSH

VRF aware TACACS+

VRF aware DNS Support

VSLP Fast Hello

VSS support for Asymmetric chassis

New and Modified IOS Software Features Supported in Cisco IOS XE 3.5.0E

The following new and modified software features are supported in Cisco IOS XE Release 3.5.0E.

<u>**New Features:**</u>

eEdge integration with MACSEC

http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/15-e/san-macsec.html

DHCP Gleaning

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-e/dhcp-gleaning.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3e/dhcp-xe-3e-book.html

Service Discovery Gateway

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dns/configuration/15-e/dns-15-e-book.html

802.1X support for trunk ports

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_8021x/configuration/15-e/con-fig-ieee-802x-pba.html

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3e/sec-usr-8021x-xe-3e-book.html

Enhancements/Respins:

Commented IP Access List Entries

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-e/sec-acl-comm-ipacl.html

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/xe-3e/sec-acl-comm-ipacl.html

IPv6 ACL Extensions for Hop by Hop Filtering

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-e/ip6-acl-ext-hbh.html

ACL Sequence Numbering

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-e/sec-acl-seq-num.html

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/xe-3e/sec-acl-seq-num.html

ACL Support for Filtering IP Options

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-e/sec-acl-support-filter-ip-option.html

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/xe-3e/sec-acl-support-filter-ip-option.html

ACL - TCP Flags Filtering

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-e/sec-create-filter-tcp.html

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/xe-3e/sec-create-filter-tcp.html

ACL - Named ACL Support for Noncontiguous Ports on an Access Control Entry

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-e/sec-named-acl-support-for-noncontiguous-ports.html

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/xe-3e/sec-named-acl-support-for-noncontiguous-ports.html

IP Access List Entry Sequence Numbering

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-e/sec-acl-seq-num.html

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/xe-3e/sec-acl-seq-num.html

IOS ACL Support for filtering IP Options

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-e/sec-acl-support-filter-ip-option.html

ACL syslog Correlation

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-e/sec-acl-syslog.html

IP Named Access Control List

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-e/sec-acl-named.html

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/xe-3e/sec-acl-named.html

IPv6 PACL support

http://cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-e/ip6-pacl-supp.html

Cisco Data Collection Manager

http://www.cisco.com/en/US/docs/ios-xml/ios/bsdcm/configuration/15-e/bsdcm-15-e-book.html

SNMPv3 Community MIB Support

http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/configuration/15-e/snmp-15-e-book.html

http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/configuration/xe-3e/snmp-xe-3e-book.html

NETCONF XML PI

http://www.cisco.com/en/US/docs/ios-xml/ios/cns/configuration/15-e/cns-15-e-book.html

IPv6 PIM Passive

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/15-e/ip6-mcast-pim-pass.html

HSRP aware PIM

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/15-e/imc_hsrp_aware.html

OSPFv3 ABR Type 3 LSA Filtering

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-e/iro-abr-type-3.html

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-e/iro-ospfv3-dc-ignore.html

Graceful Shutdown Support for OSPFv3

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-e/iro-ospfv3-gshutdown.html

OSPF Support for BFD over IPv4

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configura-tion/15-e/irbfd-bfd-ospf-ipv4-supp.html

BFD - VRF Support

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configuration/15-e/irbfd-vrf-supp.html

BFD - Static Route Support

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configura-tion/15-e/irbfd-bfd-static-route-supp.html

Static Route Support for BFD over IPv6

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configuration/15-e/ip6-bfd-static.html

BFD - EIGRP Support

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configuration/15-e/irbfd-bfd-eigrp-supp.html

OSPFv3 BFD

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configuration/15-e/ip6-route-bfd-ospfv3.html

TACACS+ Per VRF

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_tacacs/configura-tion/15-e/sec-usr-tacacs-15-e-book.html

SSHv2 Enhancements

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/15-e/sec-secure-shell-v2.html

Client Information Signalling Protocol (CISP)

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_8021x/configuration/15-e/sec-ieee-neat.html

OSPFv3 MIB

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-e/iro-ospfv3-mib.html

OSPF Non-stop Routing

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-e/iro-nsr-ospf.html

OSPFv3 Max-Metric Router-Lsa

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-e/ip6-route-osp-fv3-max-lsa.html

OSPFv3 VRF-Lite/PE-CE

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-e/iro-vrf-lite-pe-ce.html

VRRPv3 Protocol Support

http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/15-e/fhp-15-e-book_chap-ter_0100.html

IPv6 Source/Prefix Guard

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_fhsec/configuration/15-e/ip6f-15-e-book_chapter_0110.html

 IPv6 Router Advertisement Throttler

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_fhsec/configuration/15-e/ip6f-15-e-book_chapter_0111.html

 IPv6 Neighbor Discovery Multicast Suppress

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_fhsec/configuration/15-e/ip6-nd-mcast-supp.html

IPv6 Destination Guard

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_fhsec/configuration/15-e/ipv6-dest-guard.html

DHCPv6 Relay - Lightweight DHCPv6 Relay Agent

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-e/dhcp-ldra.html

DNS - VRF aware DNS

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dns/configuration/15-e/dns-15-e-book_chapter_01.html

 DHCPv6 - Relay chaining for Prefix Delegation

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-e/dhcp-15e-book_chapter_010.html

OSPFv3 Retransmission Limits

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/command/ospf-i1.html

 OSPFv3 RFC 3101 Support

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-e/iro-ospfv3-nssa-cfg.html

OSPF support for NSSA RFC 3101

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-e/iro-ospfv2-nssa-cfg.html

TFTP IPv6 support

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_nman/configuration/15-e/ip6-tftp-supp.html

Capabilities Manager

http://www.cisco.com/en/US/docs/ios-xml/ios/saf/configuration/15-e/saf-capman.html

Extensible Messaging Client Protocol (XMCP) 2.0

http://www.cisco.com/en/US/docs/ios-xml/ios/saf/configuration/15-e/saf-xmcp.html

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
03.5.0E	15.2(1)E

Upgrading the System Software

If you are upgrading to Cisco IOS XE Version 3.5.0E and plan to use VSS, you must upgrade your ROMMON to IOS Version 15.0(1r)SG10. Otherwise, you must upgrade your ROMMON to at least IOS Version 15.0(1r)SG2.

If dual supervisor engines 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

- Starting with Release IOS XE 3.3.0SG, 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.ffef ffff.ffff.0000 0000.00af.bcef ffff.ff00.0000 appletalk
    permit any host 65de.edfe.fefe xns-idp
    permit any any protocol-family rarp-non-ipv4
    deny   host 005e.1e5d.9f7d host 3399.e3e1.ff2c dec-spanning
    permit any any
```

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

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

CSCtg93278

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

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

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

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

  Workarounds:

  – Decrease the number of monitors.

  – Attach the same monitor to multiple targets. CSCti43798

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

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

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

  – At least 10K groups and roughly 20K mroutes exist.

– IGMP joins with source traffic transit to all the multicast groups.

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

Workaround: None. CSCti20312

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

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

  Workaround: Do not clear all mroutes at once.

  CSCtn06753

- Although you can configure subsecond PIM query intervals on Catalyst 4500 platforms, such an action represents a compromise between convergence (reaction time) and a number of other factors (number of mroutes, base line of CPU utilization, CPU speed, processing overhead per 1 m-route, etc.). You must account for those factors when configuring subsecond PIM timers. We recommend that you set the PIM query interval to a minimum of 2 seconds. By adjusting the available parameters, you can achieve flawless operation; that is, a top number of multicast routes per given convergence time on a specific setup.

- Energywise WOL is not "waking up" a PC in hibernate or standby mode.

  Workaround: None. CSCtr51014

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

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

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

  Workaround: Select an alternate destination or source port. CSCty05405

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

  Workaround: None. CSCty79236

- On the following linecards running IOS XE Release 3.2.3:

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

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

  the following restrictions apply:

  – Sub-interfaces are not supported on 1 Gigabit and Ten-Gigabit interfaces.

  – Port-channel members do not support multiple classification criteria for a QoS policy.

  – CEF is disabled automatically when uRFP is enabled and TCAM is fully utilized.

- When either the RADIUS-server test feature is enabled or RADIUS-server dead-criteria is configured, and either RADIUS-server deadtime is set to 0 or not configured, the RADIUS-server status is not properly relayed to AAA.

  Workaround: Configure both dead-criteria and deadtime.

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

  CSCtl06706

- If you use the **quick** option in the **issu changeversion** command, the following might occur:

  – Links flap for various Layer 3 protocols.

  – A traffic loss of several seconds is observed during the upgrade process.

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

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

  You will not experience this behavior with IPv4 access lists.

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

- Routed packets that are fragmented are not policed if the egress interface is on the VSS Standby switch. However, if the egress interface is on the VSS Active switch, these packets are policed.

  This applies to QoS policing only. QoS marking, shaping and sharing behave as expected.

  Workaround: None. CSCub14402

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

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

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

  Workaround: None. CSCua87538

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

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

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

  Workaround: None. CSCuc77376

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

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

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

  Workaround: None. CSCuf86375

- Setting a cos value based on QoS group triggers the following error message in a VSS system

  ```
  set action fail = 9
  ```

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

- Auto negotiation cannot be disabled on the Fa1 port. It must be set to auto/auto, or fixed speed with duplex auto.

- The following messages are seen during boot up after POST check.

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

  Image load status: 0x00000000
  #####
  Snowtrooper 220 controller 0x0430006E..0x044E161D Size:0x0057B4C5 Program Done!
  #########################
  ```

```
[ 6642.974087] pci 0000:00:00.0: ignoring class b20 (doesn't match header type 01)
Starting System Services
Calculating module dependencies ...
Loading rtc-ds1307
RTNETLINK answers: Invalid argument
No Mountpoints DefinedJan 17 09:48:14 %IOSXE-3-PLATFORM: process sshd[5241]: error:
Bind to port

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

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

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

Workaround: None CSCue15724

Caveats

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

> **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

Open Caveats for Cisco IOS XE Release 3.5.3E

- 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

- 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 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

- 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.   CSCub63571

- 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

- 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

- 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

- Sometimes, after VSS comes up, the control links display different VSL links.

  Workaround: Convert the VSS member switch to standalone and bring up VSS again. CSCug86547

- An IPv6 BFD session flaps if you configure a 100 * 3 timer value.

  Workaround: Set the BFD timer and multiplier as 100 * 5. CSCuh35017

- BFD supports 300ms and time values exceeding (100 * 3).

  Workaround: None. CSCuh19345

- Policer and Classification statistics do not increment during ISSU runversion when you downgrade from IOS Release XE 3.5.0E.

  Workaround: This issue is transient. Policer and Classification statistics are available after ISSU completes. CSCuh90975

- When a queuing policy is applied to a Layer 3 MEC member port, queuing statistics do not increment.

  Workaround: None CSCuh76328

- In a VSS (virtual switching system) setup, the **show switch virtual link** EXEC command displays VSL control link port numbers on different VSLs (virtual switching links) rather then displaying port numbers on the same link.

  Workaround: Convert the VSS to a standalone setup. CSCug86547

- A switch crashes when the you enter the **show power inline module 1** and **show power inline module 1 detail** commands in two different telnet sessions and reset the linecard using a third telnet session.

  Workaround: Reset the term length to 0 on the vty session. CSCuf08112

- Occasionally, when the VSL goes down on a VSS with fast-hello based dual-active detection, the Layer 2 convergence time exceeds the Layer 2 convergence time observed with e-pagp based dual-active detection by 20ms.

However, the Layer 2 convergence time of the former stills meet the sub-second convergence criteria.

Workaround: None. CSCui25034

- The **show memory debug leak** command is unavailable.

  Workaround: Use the **show memory detailed process iosd debug leaks** command. CSCui69486

- If you configure SNMP proxy and immediately remove it, your switch crashes.

  Workaround: Wait two min before removing the proxy. CSCug69823

- FHS entries do not go down during a VSS switchover

  Workaround: None. CSCub10404

- CPU utilization rises and the console may hang on simultaneously executing the following commands from either two VTY's session, or from a Console and a VTY session.

  ```
  show proc cpu <sorted|detailed|history>
  show redundancy <>
  show tech-support
  ```

  Workaround: Execute these commands in a single session.

  If you plan to execute those commands sequencially, close the console session before executing the **show tech-support** command. CSCuh15561

- The **match application name** and **collect application name** commands appear as available for flow record configuration (e.g., when using the **?** help listings). However, this configuration is otherwise unsupported: the **show flow monitor** *monitor-name* **cache** command shows the application name as 'unknown,' and the application table is not exported, so this field cannot be decoded when exported.

  Workaround: Do not configure the application name field as a key or non-key field of a flow record. CSCue47944

- If no vlan.dat exists on both source and destination, the **sync** command fails (i.e., the synchronization between flash to sdflash or sdflash to flash doesn't happen).

  Workarounds:

  - Skip the vlan.dat check.

  - Rename any config.text files as vlan.dat file. CSCue61001

- On configuring **power inline consumption**, the **show power inline** command might not display the values of the power consumed by the PD.

  Workaround: **Shut** then **no shut** the interface. CSCue72897

- On a Supervisor Engine 7L-E running IOS Release XE 3.5.0 SG, IPv6 access-list counters are not incremented when you apply a policy-map associated with a class-map matching a v6 ACL to a physical interface and send matching traffic.

  ```
  Switch# sh ipv6 access-list v6acl
  IPv6 access list v6acl
      permit ipv6 host 2003::2 any (1000 matches) sequence 10   --- only 1000 matched
  although 2000 matching pkts sent
      permit ipv6 host 2004::2 any sequence 20
  ```

  Workaround: None. CSCug54690

- While either performing an ISSU upgrade from XE 3.4.0 (or earlier) to XE 3.5.0 or performing a downgrade from XE 3.5.0 to an earlier release, the following authmgr mtu mismatch error messages might display:

```
Feb  1 09:19:05.003: %ISSU-4-FSM_INCOMP: STANDBY:Version of local ISSU client ISSU
auth mgr client(2072) in session 45 is incompatible with remote side.
Feb  1 01:22:42.159 PST: %ISSU-4-FSM_INCOMP: Version of local ISSU client ISSU auth
mgr client(2072) in session 65582 is incompatible with remote side.
Feb  1 09:22:42.139: %ISSU-3-FSM_MISMATCH_MTU: STANDBY:ISSU nego failed for client
ISSU auth mgr client(2072) entity_id 1 session 48 due to mismatch of mtu size 32 & 28.
-Traceback= 112D0D64z 1037ACE8z 126EF748z 126EF7B4z 1037BB60z 1037BBD4z 1037CB10z
10167378z 1016ACBCz 110C87FCz 110D26D4z 110D29A0z 110CE92Cz 10D4BAFCz 10D45E50z
Feb  1 09:22:42.163: %ISSU-4-FSM_INCOMP: STANDBY:Version of local ISSU client ISSU
auth mgr client(2072) in session 48 is incompatible with remote side.
```

These messages does not impact ISSU processing.

These messages may be seen on both VSS and standalone topologies.

Workaround: None CSCue37937

- Flexible NetFlow configured to **collect transport tcp flags** may not collect these flags from all segments in a flow.

  Workaround: Add the following to the relevant flow record configuration:

  collect{ipv4 | ipv6} length total

  match{ipv4 | ipv6} protocol.

  CSCue02484

- The **match application name** and **collect application name** commands appear available for flow record configuration when you use the **?** help listings. However, the following configuration is otherwise unsupported: **show flow monitor** *i* **monitor-name** *i* **cache** displays the application name as "unknown;" and the application table is not exported. So, the application name field cannot be decoded when exported.

  Workaround: Do not configure the application name field as a key or non-key field of a flow record.

  CSCue47944

- While performing an ISSU upgrade from a prior release (like upgrading IOS Release XE 3.3.0SG (or 3.4.0SG) to 3.5.0SG) the following message are displayed several times on the switch console:

  ```
  %CTS-3-MSG_NOT_COMPATIBLE_WITH_PEER: STANDBY:Message 2 in component 3 is not
  compatible with the peer.
  ```

  This does not impact functionality.

  Workaround: None. CSCuh47387

- When VSL encryption is enabled and linecard ports are configured as VSL, an OIR may cause a switch to crash.

  Workaround: Shut the individual VSL ports then perform an OIR.CSCuh98510

- When a command's paginated output is sent into a pipe on a switch using VSS, console control is not returned.

  Workarounds:

  1. Use terminal length 0 to turn off pagination.

  2. Use any key other than Enter or Space. CSCui44781

- While performing an ISSU from IOS Release XE 3.5.0E to 3.3.2.SG, the following message is observed:

  ```
  SW_LEVEL-6-RESULT: Operational redundancy mode is UNKNOWN, due to software
  license-level mismatch at ACTIVE and STANDBY. Software Level on Active: entservices;
  on Standby: entservices.
  ```

     Workaround: None. CSCui54147

- IPv6 Source Guard does not block packets from IP sources that are not in the binding table.

  Workaround: None CSCug79180

- Cisco TrustSec/MacSec support for WS-X4748-SFP-E, WS-X4724-SFP-E, and WS-X4712-SFP-E linecards is limited to the following:

  - CTS support for SXP

  - Cisco TrustSec Switch-to-Switch Link Security in 802.1X and manual modes.

- If BFD sessions are hardware offloaded in a VSS, BFD sessions undergo re-negotiation after a VSS switchover.

  Workaround: None. CSCug62308

- If BFD is configured in a VSS, BFD sessions flap after a VSS switchover.

  Workaround: Issue the bfd interval 999 min_rx 999 multiplier 6 command on the interface participating in the BFD session. CSCuh16490

- When the standby of a VSS system reloads and the CTS links are in **no shutdown** state, the CTS links on the standby are stuck in AUTHEN state..

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command. CSCuv15017

- After kron performs a write of the startup-config (e.g. 'write mem'), it is locked indefinitely (i.e., the startup-config and running-config are unavailable):

  ```
  switch# show run
  Unable to get configuration. Try again later.
  ```

  Workaround; Reload the switch.

  To avoid this condition, use EEM with the timer event to schedule the required task.

  CSCtk68692

Resolved Caveats for Cisco IOS XE Release 3.5.3E

- Power-on self-test (POST) requires more than two minutes to execute.

  Workaround: None

  This issue applies only to Supervisor Engine 7L-E.

  CSCuo45044

Open Caveats for Cisco IOS XE Release 3.5.2E

- 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

- 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 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

- 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.   CSCub63571

- 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

- 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

- 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

- Sometimes, after VSS comes up, the control links display different VSL links.

  Workaround: Convert the VSS member switch to standalone and bring up VSS again. CSCug86547

- An IPv6 BFD session flaps if you configure a 100 * 3 timer value.

  Workaround: Set the BFD timer and multiplier as 100 * 5. CSCuh35017

- BFD supports 300ms and time values exceeding (100 * 3).

  Workaround: None. CSCuh19345

- Policer and Classification statistics do not increment during ISSU runversion when you downgrade from IOS Release XE 3.5.0E.

  Workaround: This issue is transient. Policer and Classification statistics are available after ISSU completes. CSCuh90975

- When a queuing policy is applied to a Layer 3 MEC member port, queuing statistics do not increment.

  Workaround: None CSCuh76328

- In a VSS (virtual switching system) setup, the **show switch virtual link** EXEC command displays VSL control link port numbers on different VSLs (virtual switching links) rather then displaying port numbers on the same link.

  Workaround: Convert the VSS to a standalone setup. CSCug86547

- A switch crashes when the you enter the **show power inline module 1** and **show power inline module 1 detail** commands in two different telnet sessions and reset the linecard using a third telnet session.

  Workaround: Reset the term length to 0 on the vty session. CSCuf08112

- Occasionally, when the VSL goes down on a VSS with fast-hello based dual-active detection, the Layer 2 convergence time exceeds the Layer 2 convergence time observed with e-pagp based dual-active detection by 20ms.

  However, the Layer 2 convergence time of the former stills meet the sub-second convergence criteria.

  Workaround: None. CSCui25034

- The **show memory debug leak** command is unavailable.

  Workaround: Use the **show memory detailed process iosd debug leaks** command. CSCui69486

- If you configure SNMP proxy and immediately remove it, your switch crashes.

  Workaround: Wait two min before removing the proxy. CSCug69823

- FHS entries do not go down during a VSS switchover

  Workaround: None. CSCub10404

- CPU utilization rises and the console may hang on simultaneously executing the following commands from either two VTY's session, or from a Console and a VTY session.

  ```
  show proc cpu <sorted|detailed|history>
  show redundancy <>
  show tech-support
  ```

  Workaround: Execute these commands in a single session.

  If you plan to execute those commands sequencially, close the console session before executing the **show tech-support** command. CSCuh15561

- The **match application name** and **collect application name** commands appear as available for flow record configuration (e.g., when using the **?** help listings). However, this configuration is otherwise unsupported: the **show flow monitor** *monitor-name* **cache** command shows the application name as 'unknown,' and the application table is not exported, so this field cannot be decoded when exported.

  Workaround: Do not configure the application name field as a key or non-key field of a flow record. CSCue47944

- If no vlan.dat exists on both source and destination, the **sync** command fails (i.e., the synchronization between flash to sdflash or sdflash to flash doesn't happen).

  Workarounds:

  - Skip the vlan.dat check.

  - Rename any config.text files as vlan.dat file. CSCue61001

- On configuring **power inline consumption**, the **show power inline** command might not display the values of the power consumed by the PD.

  Workaround: **Shut** then **no shut** the interface. CSCue72897

- On a Supervisor Engine 7L-E running IOS Release XE 3.5.0 SG, IPv6 access-list counters are not incremented when you apply a policy-map associated with a class-map matching a v6 ACL to a physical interface and send matching traffic.

```
Switch# sh ipv6 access-list v6acl
IPv6 access list v6acl
    permit ipv6 host 2003::2 any (1000 matches) sequence 10    --- only 1000 matched
although 2000 matching pkts sent
    permit ipv6 host 2004::2 any sequence 20
```

  Workaround: None. CSCug54690

- While either performing an ISSU upgrade from XE 3.4.0 (or earlier) to XE 3.5.0 or performing a downgrade from XE 3.5.0 to an earlier release, the following authmgr mtu mismatch error messages might display:

```
Feb  1 09:19:05.003: %ISSU-4-FSM_INCOMP: STANDBY:Version of local ISSU client ISSU
auth mgr client(2072) in session 45 is incompatible with remote side.
Feb  1 01:22:42.159 PST: %ISSU-4-FSM_INCOMP: Version of local ISSU client ISSU auth
mgr client(2072) in session 65582 is incompatible with remote side.
Feb  1 09:22:42.139: %ISSU-3-FSM_MISMATCH_MTU: STANDBY:ISSU nego failed for client
ISSU auth mgr client(2072) entity_id 1 session 48 due to mismatch of mtu size 32 & 28.
-Traceback= 112D0D64z 1037ACE8z 126EF748z 126EF7B4z 1037BB60z 1037BBD4z 1037CB10z
10167378z 1016ACBCz 110C87FCz 110D26D4z 110D29A0z 110CE92Cz 10D4BAFCz 10D45E50z
Feb  1 09:22:42.163: %ISSU-4-FSM_INCOMP: STANDBY:Version of local ISSU client ISSU
auth mgr client(2072) in session 48 is incompatible with remote side.
```

  These messages does not impact ISSU processing.

  These messages may be seen on both VSS and standalone topologies.

  Workaround: None CSCue37937

- Flexible NetFlow configured to **collect transport tcp flags** may not collect these flags from all segments in a flow.

  Workaround: Add the following to the relevant flow record configuration:

  collect{**ipv4** | **ipv6**} **length total**

  match{**ipv4** | **ipv6**} **protocol**.

  CSCue02484

- The **match application name** and **collect application name** commands appear available for flow record configuration when you use the **?** help listings. However, the following configuration is otherwise unsupported: **show flow monitor** *i* **monitor-name** *i* **cache** displays the application name as "unknown;" and the application table is not exported. So, the application name field cannot be decoded when exported.

  Workaround: Do not configure the application name field as a key or non-key field of a flow record.

  CSCue47944

- While performing an ISSU upgrade from a prior release (like upgrading IOS Release XE 3.3.0SG (or 3.4.0SG) to 3.5.0SG) the following message are displayed several times on the switch console:

```
%CTS-3-MSG_NOT_COMPATIBLE_WITH_PEER: STANDBY:Message 2 in component 3 is not
compatible with the peer.
```

  This does not impact functionality.

  Workaround: None. CSCuh47387

- When VSL encryption is enabled and linecard ports are configured as VSL, an OIR may cause a switch to crash.

Workaround: Shut the individual VSL ports then perform an OIR.CSCuh98510

- When a command's paginated output is sent into a pipe on a switch using VSS, console control is not returned.

  Workarounds:

  1. Use terminal length 0 to turn off pagination.

  2. Use any key other than Enter or Space. CSCui44781

- While performing an ISSU from IOS Release XE 3.5.0E to 3.3.2.SG, the following message is observed:

  ```
  SW_LEVEL-6-RESULT: Operational redundancy mode is UNKNOWN, due to software
  license-level mismatch at ACTIVE and STANDBY. Software Level on Active: entservices;
  on Standby: entservices.
  ```

  Workaround: None. CSCui54147

- IPv6 Source Guard does not block packets from IP sources that are not in the binding table.

  Workaround: None CSCug79180

- Cisco TrustSec/MacSec support for WS-X4748-SFP-E, WS-X4724-SFP-E, and WS-X4712-SFP-E linecards is limited to the following:

  – CTS support for SXP

  – Cisco TrustSec Switch-to-Switch Link Security in 802.1X and manual modes.

- If BFD sessions are hardware offloaded in a VSS, BFD sessions undergo re-negotiation after a VSS switchover.

  Workaround: None. CSCug62308

- If BFD is configured in a VSS, BFD sessions flap after a VSS switchover.

  Workaround: Issue the bfd interval 999 min_rx 999 multiplier 6 command on the interface participating in the BFD session. CSCuh16490

- After kron performs a write of the startup-config (e.g. 'write mem'), it is locked indefinitely (i.e., the startup-config and running-config are unavailable):

  ```
  switch# show run
  Unable to get configuration. Try again later.
  ```

  Workaround; Reload the switch.

  To avoid this condition, use EEM with the timer event to schedule the required task.

  CSCtk68692

Resolved Caveats for Cisco IOS XE Release 3.5.2E

- On a switch running Cisco IOS XE 3.5.1E, issuing a **show** command causes a vty / console session to hang; the prompt does not return.

  Workarounds:

  – If an unused VTY session exists, issue the **clear vty** *option* or **clear line** *vty-name* command.

  – Avoid issuing commands with huge outputs. CSCul95289

- mDNS malformed packets cause the switch to crash during normal network operation.

  Workaround: None. CSCul90866

Open Caveats for Cisco IOS XE Release 3.5.1E

- 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

- 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 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

- 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.   CSCub63571

- 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

- 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

- 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

- Sometimes, after VSS comes up, the control links display different VSL links.

    Workaround: Convert the VSS member switch to standalone and bring up VSS again. CSCug86547

- An IPv6 BFD session flaps if you configure a 100 * 3 timer value.

    Workaround: Set the BFD timer and multiplier as 100 * 5. CSCuh35017

- BFD supports 300ms and time values exceeding (100 * 3).

    Workaround: None. CSCuh19345

- Policer and Classification statistics do not increment during ISSU runversion when you downgrade from IOS Release XE 3.5.0E.

Workaround: This issue is transient. Policer and Classification statistics are available after ISSU completes. CSCuh90975

- When a queuing policy is applied to a Layer 3 MEC member port, queuing statistics do not increment.

    Workaround: None CSCuh76328

- In a VSS (virtual switching system) setup, the **show switch virtual link** EXEC command displays VSL control link port numbers on different VSLs (virtual switching links) rather then displaying port numbers on the same link.

    Workaround: Convert the VSS to a standalone setup. CSCug86547

- A switch crashes when the you enter the **show power inline module 1** and **show power inline module 1 detail** commands in two different telnet sessions and reset the linecard using a third telnet session.

    Workaround: Reset the term length to 0 on the vty session. CSCuf08112

- Occasionally, when the VSL goes down on a VSS with fast-hello based dual-active detection, the Layer 2 convergence time exceeds the Layer 2 convergence time observed with e-pagp based dual-active detection by 20ms.

    However, the Layer 2 convergence time of the former stills meet the sub-second convergence criteria.

    Workaround: None. CSCui25034

- The **show memory debug leak** command is unavailable.

    Workaround: Use the **show memory detailed process iosd debug leaks** command. CSCui69486

- If you configure SNMP proxy and immediately remove it, your switch crashes.

    Workaround: Wait two min before removing the proxy. CSCug69823

- FHS entries do not go down during a VSS switchover

    Workaround: None. CSCub10404

- CPU utilization rises and the console may hang on simultaneously executing the following commands from either two VTY's session, or from a Console and a VTY session.

    ```
    show proc cpu <sorted|detailed|history>
    show redundancy <>
    show tech-support
    ```

    Workaround: Execute these commands in a single session.

    If you plan to execute those commands sequentially, close the console session before executing the **show tech-support** command. CSCuh15561

- The **match application name** and **collect application name** commands appear as available for flow record configuration (e.g., when using the **?** help listings). However, this configuration is otherwise unsupported: the **show flow monitor** *monitor-name* **cache** command shows the application name as 'unknown,' and the application table is not exported, so this field cannot be decoded when exported.

    Workaround: Do not configure the application name field as a key or non-key field of a flow record. CSCue47944

- If no vlan.dat exists on both source and destination, the **sync** command fails (i.e., the synchronization between flash to sdflash or sdflash to flash doesn't happen).

    Workarounds:

    - Skip the vlan.dat check.

- – Rename any config.text files as vlan.dat file. CSCue61001

- On configuring **power inline consumption**, the **show power inline** command might not display the values of the power consumed by the PD.

  Workaround: **Shut** then **no shut** the interface. CSCue72897

- On a Supervisor Engine 7L-E running IOS Release XE 3.5.0 SG, IPv6 access-list counters are not incremented when you apply a policy-map associated with a class-map matching a v6 ACL to a physical interface and send matching traffic.

  ```
  Switch# sh ipv6 access-list v6acl
  IPv6 access list v6acl
      permit ipv6 host 2003::2 any (1000 matches) sequence 10   --- only 1000 matched
  although 2000 matching pkts sent
      permit ipv6 host 2004::2 any sequence 20
  ```

  Workaround: None. CSCug54690

- While either performing an ISSU upgrade from XE 3.4.0 (or earlier) to XE 3.5.0 or performing a downgrade from XE 3.5.0 to an earlier release, the following authmgr mtu mismatch error messages might display:

  ```
  Feb  1 09:19:05.003: %ISSU-4-FSM_INCOMP: STANDBY:Version of local ISSU client ISSU
  auth mgr client(2072) in session 45 is incompatible with remote side.
  Feb  1 01:22:42.159 PST: %ISSU-4-FSM_INCOMP: Version of local ISSU client ISSU auth
  mgr client(2072) in session 65582 is incompatible with remote side.
  Feb  1 09:22:42.139: %ISSU-3-FSM_MISMATCH_MTU: STANDBY:ISSU nego failed for client
  ISSU auth mgr client(2072) entity_id 1 session 48 due to mismatch of mtu size 32 & 28.
  -Traceback= 112D0D64z 1037ACE8z 126EF748z 126EF7B4z 1037BB60z 1037BBD4z 1037CB10z
  10167378z 1016ACBCz 110C87FCz 110D26D4z 110D29A0z 110CE92Cz 10D4BAFCz 10D45E50z
  Feb  1 09:22:42.163: %ISSU-4-FSM_INCOMP: STANDBY:Version of local ISSU client ISSU
  auth mgr client(2072) in session 48 is incompatible with remote side.
  ```

  These messages does not impact ISSU processing.

  These messages may be seen on both VSS and standalone topologies.

  Workaround: None CSCue37937

- Flexible NetFlow configured to **collect transport tcp flags** may not collect these flags from all segments in a flow.

  Workaround: Add the following to the relevant flow record configuration:

  collect{**ipv4** | **ipv6**} **length total**

  match{**ipv4** | **ipv6**} **protocol**.

  CSCue02484

- The **match application name** and **collect application name** commands appear available for flow record configuration when you use the **?** help listings. However, the following configuration is otherwise unsupported: **show flow monitor** *i* **monitor-name** *i* **cache** displays the application name as "unknown;" and the application table is not exported. So, the application name field cannot be decoded when exported.

  Workaround: Do not configure the application name field as a key or non-key field of a flow record.

  CSCue47944

- While performing an ISSU upgrade from a prior release (like upgrading IOS Release XE 3.3.0SG (or 3.4.0SG) to 3.5.0SG) the following message are displayed several times on the switch console:

  ```
  %CTS-3-MSG_NOT_COMPATIBLE_WITH_PEER: STANDBY:Message 2 in component 3 is not
  compatible with the peer.
  ```

This does not impact functionality.

Workaround: None. CSCuh47387

- When VSL encryption is enabled and linecard ports are configured as VSL, an OIR may cause a switch to crash.

  Workaround: Shut the individual VSL ports then perform an OIR.CSCuh98510

- When a command's paginated output is sent into a pipe on a switch using VSS, console control is not returned.

  Workarounds:

  1. Use terminal length 0 to turn off pagination.

  2. Use any key other than Enter or Space. CSCui44781

- While performing an ISSU from IOS Release XE 3.5.0E to 3.3.2.SG, the following message is observed:

  ```
  SW_LEVEL-6-RESULT: Operational redundancy mode is UNKNOWN, due to software
  license-level mismatch at ACTIVE and STANDBY. Software Level on Active: entservices;
  on Standby: entservices.
  ```

  Workaround: None. CSCui54147

- IPv6 Source Guard does not block packets from IP sources that are not in the binding table.

  Workaround: None CSCug79180

- Cisco TrustSec/MacSec support for WS-X4748-SFP-E, WS-X4724-SFP-E, and WS-X4712-SFP-E linecards is limited to the following:

  - CTS support for SXP

  - Cisco TrustSec Switch-to-Switch Link Security in 802.1X and manual modes.

- If BFD sessions are hardware offloaded in a VSS, BFD sessions undergo re-negotiation after a VSS switchover.

  Workaround: None. CSCug62308

- If BFD is configured in a VSS, BFD sessions flap after a VSS switchover.

  Workaround: Issue the bfd interval 999 min_rx 999 multiplier 6 command on the interface participating in the BFD session. CSCuh16490

- After kron performs a write of the startup-config (e.g. 'write mem'), it is locked indefinitely (i.e., the startup-config and running-config are unavailable):

  ```
  switch# show run
  Unable to get configuration. Try again later.
  ```

  Workaround; Reload the switch.

  To avoid this condition, use EEM with the timer event to schedule the required task.

  CSCtk68692

Resolved Caveats for Cisco IOS XE Release 3.5.1E

- If **login quiet-mode** is configured, a switch resets when you enter the **no login block-for** command.

  Workaround: None.

  CSCts80209

- Provided an HTTP server is enabled on a switch, a vulnerability exists in Cisco IOS switches where the remote, non-authenticated attacker can cause Denial of Service (DoS) by reloading an affected device.

  An attacker can exploit this vulnerability by sending a special combination of crafted packets.

  Workaround: None

  PSIRT Evaluation:

  The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.2:

  http://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?

  dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:POC/RL:OF/RC:C

  CVE ID CVE-2013-1100 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at:

  http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-1100

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

  CSCuc53853

- When you enable either the device-sensor accounting or the access-session accounting attributes command, the accounting request itself is not sent from the switch to the radius (ISE) Server.

  Workaround: Do not enable device-sensor accounting.

  The user accounting message will not carry the device-sensor attributes to the ISE.

  CSCuj56845

- When the same ACL is installed on two ports of a switch and a user is unauthenticated or logged out, the ACS-configured dynamic ACLs are not applied or deleted from the port.

  Workaround: None CSCuj99722

- 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

- If you issue the **show platform cpu packet driver** command multiple times, ARP, IGMP and other control protocols cease processing and the following output displays:

```
#show platform cpu packet driver
Forerunner Packet Engine 0.28 (0)
Receive Queues: received packets summary
Qu  Capac  Guara  CurPo  Unpro  Accum   Kept  BperP            Packets<br>
 2   2512    112   2303      0      3   2511    64                339959 <--- Kept stays
at 2511, Packets does not increment
 8   1008    512     67      0      3      3    64                    67
 9   2512    304     96      0      0      0   433                    96
Receive Queues: dropped packets summary
Qu     Total Packets      Drop No Cell     Drop Overrun    Drop Underrun
```

```
   2          339959          100390067                      0                  0 <--- Drop
No Cell increments
```

Workarounds:

- **–** Do not use vlan 1.

- **–** Toggle **ipv6 snooping** ON and OFF again under "vlan configuration 1" soon after bootup.

CSCuj73571

- A Dynamic ACL with a remark statement is not pushed from ISE to client and authorization either fails or is unauthorized.

Workaround: Remove the remark statement from the DACL. CSCuj35704

- The temperature thresholds for WS-X4748-SFP-E, WS-X4724-SFP-E, and WS-X4712-SFP-E linecards are set too low:

```
Incorrect values:
Sensor              (warning, critical, shutdown)
Air inlet           (44C,59C,62C)
Air inlet remote    (47C,61C,64C)
Air outlet          (47C,62C,65C)
Air outlet remote   (52C,66C,69C)

Correct values:
Air inlet           (47C,61C,64C)
Air inlet remote    (54C,66C,69C)
Air outlet          (55C,67C,70C)
Air outlet remote   (65C,76C,79C)
```

This behavior causes false warnings or linecard failure errors, as follows:

```
*Oct 29 07:40:38.858: %C4K_IOSMODPORTMAN-2-MODULECRITICALTEMP: Module 8 Sensor Air
outlet temperature is at or over critical threshold - current temp: 62C, critical
threshold: 62C

*Oct 29 07:40:38.690: %C4K_IOSMODPORTMAN-2-MODULESHUTDOWNTEMP: Module 1 Sensor Air
inlet remote temperature is at or over shutdown threshold - current temp: 64C,
shutdown threshold: 64C
```

Workaround: None. CSCul13858

Open Caveats for Cisco IOS XE Release 3.5.0E

- 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

- 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 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

- 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. CSCub63571

- 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

- 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

- 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

- Sometimes, after VSS comes up, the control links display different VSL links.

  Workaround: Convert the VSS member switch to standalone and bring up VSS again. CSCug86547

- An IPv6 BFD session flaps if you configure a 100 * 3 timer value.

  Workaround: Set the BFD timer and multiplier as 100 * 5. CSCuh35017

- BFD supports 300ms and time values exceeding (100 * 3).

  Workaround: None. CSCuh19345

- Policer and Classification statistics do not increment during ISSU runversion when you downgrade from IOS Release XE 3.5.0E.

  Workaround: This issue is transient. Policer and Classification statistics are available after ISSU completes. CSCuh90975

- When a queuing policy is applied to a Layer 3 MEC member port, queuing statistics do not increment.

  Workaround: None CSCuh76328

- In a VSS (virtual switching system) setup, the **show switch virtual link** EXEC command displays VSL control link port numbers on different VSLs (virtual switching links) rather then displaying port numbers on the same link.

  Workaround: Convert the VSS to a standalone setup. CSCug86547

- A switch crashes when the you enter the **show power inline module 1** and **show power inline module 1 detail** commands in two different telnet sessions and reset the linecard using a third telnet session.

  Workaround: Reset the term length to 0 on the vty session. CSCuf08112

- Occasionally, when the VSL goes down on a VSS with fast-hello based dual-active detection, the Layer 2 convergence time exceeds the Layer 2 convergence time observed with e-pagp based dual-active detection by 20ms.

  However, the Layer 2 convergence time of the former stills meet the sub-second convergence criteria.

  Workaround: None. CSCui25034

- The **show memory debug leak** command is unavailable.

  Workaround: Use the **show memory detailed process iosd debug leaks** command. CSCui69486

- If you configure SNMP proxy and immediately remove it, your switch crashes.

  Workaround: Wait two min before removing the proxy. CSCug69823

- FHS entries do not go down during a VSS switchover

  Workaround: None. CSCub10404

- CPU utilization rises and the console may hang on simultaneously executing the following commands from either two VTY's session, or from a Console and a VTY session.

  ```
  show proc cpu <sorted|detailed|history>
  show redundancy <>
  show tech-support
  ```

  Workaround: Execute these commands in a single session.

  If you plan to execute those commands sequencially, close the console session before executing the **show tech-support** command. CSCuh15561

- The **match application name** and **collect application name** commands appear as available for flow record configuration (e.g., when using the **?** help listings). However, this configuration is otherwise unsupported: the **show flow monitor** *monitor-name* **cache** command shows the application name as 'unknown,' and the application table is not exported, so this field cannot be decoded when exported.

  Workaround: Do not configure the application name field as a key or non-key field of a flow record. CSCue47944

- If no vlan.dat exists on both source and destination, the **sync** command fails (i.e., the synchronization between flash to sdflash or sdflash to flash doesn't happen).

  Workarounds:

  - Skip the vlan.dat check.
  - Rename any config.text files as vlan.dat file. CSCue61001

- On configuring **power inline consumption**, the **show power inline** command might not display the values of the power consumed by the PD.

  Workaround: **Shut** then **no shut** the interface. CSCue72897

- On a Supervisor Engine 7L-E running IOS Release XE 3.5.0 SG, IPv6 access-list counters are not incremented when you apply a policy-map associated with a class-map matching a v6 ACL to a physical interface and send matching traffic.

  ```
  Switch# sh ipv6 access-list v6acl
  IPv6 access list v6acl
      permit ipv6 host 2003::2 any (1000 matches) sequence 10   --- only 1000 matched
  although 2000 matching pkts sent
      permit ipv6 host 2004::2 any sequence 20
  ```

  Workaround: None. CSCug54690

- While either performing an ISSU upgrade from XE 3.4.0 (or earlier) to XE 3.5.0 or performing a downgrade from XE 3.5.0 to an earlier release, the following authmgr mtu mismatch error messages might display:

```
Feb  1 09:19:05.003: %ISSU-4-FSM_INCOMP: STANDBY:Version of local ISSU client ISSU
auth mgr client(2072) in session 45 is incompatible with remote side.
Feb  1 01:22:42.159 PST: %ISSU-4-FSM_INCOMP: Version of local ISSU client ISSU auth
mgr client(2072) in session 65582 is incompatible with remote side.
Feb  1 09:22:42.139: %ISSU-3-FSM_MISMATCH_MTU: STANDBY:ISSU nego failed for client
ISSU auth mgr client(2072) entity_id 1 session 48 due to mismatch of mtu size 32 & 28.
-Traceback= 112D0D64z 1037ACE8z 126EF748z 126EF7B4z 1037BB60z 1037BBD4z 1037CB10z
10167378z 1016ACBCz 110C87FCz 110D26D4z 110D29A0z 110CE92Cz 10D4BAFCz 10D45E50z
Feb  1 09:22:42.163: %ISSU-4-FSM_INCOMP: STANDBY:Version of local ISSU client ISSU
auth mgr client(2072) in session 48 is incompatible with remote side.
```

  These messages does not impact ISSU processing.

  These messages may be seen on both VSS and standalone topologies.

  Workaround: None CSCue37937

- Flexible NetFlow configured to **collect transport tcp flags** may not collect these flags from all segments in a flow.

  Workaround: Add the following to the relevant flow record configuration:

  collect{**ipv4** | **ipv6**} **length total**

  match{**ipv4** | **ipv6**} **protocol**.

  CSCue02484

- The **match application name** and **collect application name** commands appear available for flow record configuration when you use the **?** help listings. However, the following configuration is otherwise unsupported: **show flow monitor** *i* **monitor-name** *i* **cache** displays the application name as "unknown;" and the application table is not exported. So, the application name field cannot be decoded when exported.

  Workaround: Do not configure the application name field as a key or non-key field of a flow record.

  CSCue47944

- While performing an ISSU upgrade from a prior release (like upgrading IOS Release XE 3.3.0SG (or 3.4.0SG) to 3.5.0SG) the following message are displayed several times on the switch console:

```
%CTS-3-MSG_NOT_COMPATIBLE_WITH_PEER: STANDBY:Message 2 in component 3 is not
compatible with the peer.
```

  This does not impact functionality.

  Workaround: None. CSCuh47387

- When VSL encryption is enabled and linecard ports are configured as VSL, an OIR may cause a switch to crash.

  Workaround: Shut the individual VSL ports then perform an OIR.CSCuh98510

- When a command's paginated output is sent into a pipe on a switch using VSS, console control is not returned.

  Workarounds:

  1. Use terminal length 0 to turn off pagination.

  2. Use any key other than Enter or Space. CSCui44781

- While performing an ISSU from IOS Release XE 3.5.0E to 3.3.2.SG, the following message is observed:

```
SW_LEVEL-6-RESULT: Operational redundancy mode is UNKNOWN, due to software
license-level mismatch at ACTIVE and STANDBY. Software Level on Active: entservices;
on Standby: entservices.
```

Workaround: None. CSCui54147

- IPv6 Source Guard does not block packets from IP sources that are not in the binding table.

Workaround: None CSCug79180

- 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

- The temperature thresholds for WS-X4748-SFP-E, WS-X4724-SFP-E, and WS-X4712-SFP-E linecards are set too low:

```
Incorrect values:
Sensor              (warning, critical, shutdown)
Air inlet           (44C,59C,62C)
Air inlet remote    (47C,61C,64C)
Air outlet          (47C,62C,65C)
Air outlet remote   (52C,66C,69C)

Correct values:
Air inlet           (47C,61C,64C)
Air inlet remote    (54C,66C,69C)
Air outlet          (55C,67C,70C)
Air outlet remote   (65C,76C,79C)
```

This behavior causes false warnings or linecard failure errors, as follows:

```
*Oct 29 07:40:38.858: %C4K_IOSMODPORTMAN-2-MODULECRITICALTEMP: Module 8 Sensor Air
outlet temperature is at or over critical threshold - current temp: 62C, critical
threshold: 62C

*Oct 29 07:40:38.690: %C4K_IOSMODPORTMAN-2-MODULESHUTDOWNTEMP: Module 1 Sensor Air
inlet remote temperature is at or over shutdown threshold - current temp: 64C,
shutdown threshold: 64C
```

Workaround: None. CSCul13858

- If BFD sessions are hardware offloaded in a VSS, BFD sessions undergo re-negotiation after a VSS switchover.

Workaround: None. CSCug62308

- If BFD is configured in a VSS, BFD sessions flap after a VSS switchover.

Workaround: Issue the bfd interval 999 min_rx 999 multiplier 6 command on the interface participating in the BFD session. CSCuh16490

- After kron performs a write of the startup-config (e.g. 'write mem'), it is locked indefinitely (i.e., the startup-config and running-config are unavailable):

```
switch# show run
Unable to get configuration. Try again later.
```

Workaround; Reload the switch.

To avoid this condition, use EEM with the timer event to schedule the required task.

CSCtk68692

Resolved Caveats for Cisco IOS XE Release 3.5.0E

This section lists the resolved caveats for Cisco IOS XE Release 3.5.0E:

- If you configure **flowcontrol receive on/off** on an port-channel interface of Supervisor Engine 7-E, only one member interface flaps.

  Typically, all the member interfaces change their flowcontrol config so that they flap once.

  Workaround: Configure the **onminterface** command through the **range** command.

  CSCue80208

- The SNMP engine process shows high CPU, when you execute **snmpbulkget** or **snmpwalk** on the following OID:

  ```
  .1.0.8802.1.1.2.1.4.2.1.4
  .1.0.8802.1.1.2.1.4.2.1.5
  .1.0.8802.1.1.2.1.4.2.1.6
  .1.0.8802.1.1.2.1.4.2.1.7
  .1.0.8802.1.1.2.1.4.2.1.8
  ```

  Workaround: None. CSCue86626

- The active supervisor engine crashes when one of the vty sessions displays **power inline details** for a module (with **automore** enabled) and simultaneously the module is reset from the other vty session.

  Workaround: Set term length 0 on the vty sessions. CSCuf08112

- If you have a switch running MST and a second switch running RSTP, a Layer 2 loop results; MST and RSTP are not interoperable.

  The access port on the MST boundary goes into "Type inconsistent" state for MST instance 0, but not for the other instances (VLAN 100 is a member of instance 1).

  Workaround: None. CSCud67457

- When you remove or insert the fan tray, the following message appears:

  ```
  *Jan 21 07:55:08.851: %C4K_IOSMODPORTMAN-6-FANTRAYINSERTEDDETAILED: Fan tray ( S/N:
  Hw: 0.0) has been inserted
  ```

  Workaround: None. CSCue34358

- When using PEAPv1/MSChap from an IOS Supplicant to ACS 5 (and possibly other RADIUS servers), authentication fails.

  Workaround: Use PEAP-GTC or any other method. CSCud66899

- Wireshark might not capture packets egressing a port.

  Workaround: None. CSCud80251

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

Original SSLeay License:

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

This package is an SSL implementation written by Eric Young (eay@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 (eay@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].