# Release Notes for the Catalyst 4500-X Series Switches, 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 4500-X Series switch. This releases delivers 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.

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 4500-X switch, visit the following URL:

http://www.cisco.com//en/US/products/ps12332/index.html

**Note** Although their Release Notes are unique, the platforms Catalyst 4500E and Catalyst 4500-X use the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide.*

# Contents

This publication consists of these sections:

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

# Cisco IOS Software Packaging

The Enterprise Services image supports all Cisco Catalyst 4500-X 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).

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

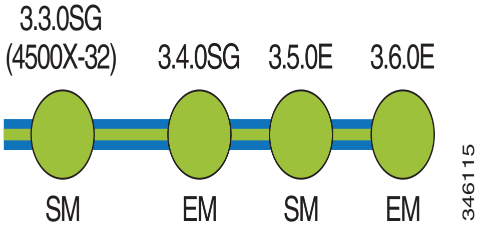
# Cisco IOS XE Release Strategy

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

IOS XE 3.4.xSG is a maintenance train supporting Sup7E, Sup7L-E and 4500-X.

Figure 1 displays the one active train, 3.4.0SG.

*Figure 1 Software Release Strategy for the Catalyst 4500-X 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 4500-X Series Switches, page 3
- Feature Support by Image Type, page 6
- MIB Support, page 26
- Features Not Supported on the Cisco Catalyst 4500-X Series Switches, page 26
- Orderable Product Numbers, page 27

## Supported Hardware on the Catalyst 4500-X Series Switches

Table 1 lists the hardware supported on the Catalyst 4500-X Series switches.

*Table 1 Supported Hardware on the Cisco Catalyst 4500-X Series Switch*

| **Product Number** (append with "=" for spares) | **Product Description** |
|---|---|
| **Small Form-Factor Pluggable Gigabit Ethernet Modules** | |
| GLC-BX-D | 1000BASE-BX10-D small form-factor pluggable module<br>For DOM support, see Table 4 on page 6. |
| GLC-BX-U | 1000BASE-BX10-U small form-factor pluggable module<br>For DOM support, see Table 4 on page 6.bv |
| 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 |
| 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-ZX-SM | 1000BASE-ZX small form-factor pluggable module |
| GLC-ZX-SMD | 1000BASE-ZX small form-factor pluggable module with DOM support |
| GLC-T | 1000BASE-T small form-factor pluggable module |
| CWDM-SFP-xxxx | CWDM small form-factor pluggable module (See Table 2 on page 4 for a list of supported wavelengths.)<br>For DOM support, see Table 4 on page 6. |
| SFP-DWDM | Dense Wavelength-Division Multiplexing (DWDM) Small Form Factor Pluggable (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 |

*Table 1 Supported Hardware on the Cisco Catalyst 4500-X Series Switch (continued)*

| **Product Number** (append with "=" for spares) | **Product Description** |
|---|---|
| | |
| 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<br>**Note** This module is only supported on the uplink module in the back-to-front airflow configuration. |

Table 2 briefly describes the supported CWDM wavelengths in the Catalyst 4500-X Series switch.

*Table 2 CWDM SFP Supported Wavelengths on the Cisco Catalyst 4500-X Series Switches*

| **Product Number** (append with "=" for spares) | **Product Description** |
|---|---|
| | |
| CWDM SFP -1470 | Longwave 1470 nm laser single-mode |
| CWDM SFP -1490 | Longwave 1490 nm laser single-mode |
| CWDM SFP -1510 | Longwave 1510 nm laser single-mode |
| CWDM SFP -1530 | Longwave 1530 nm laser single-mode |
| CWDM SFP -1550 | Longwave 1550 nm laser single-mode |
| CWDM SFP -1570 | Longwave 1570 nm laser single-mode |
| CWDM SFP -1590 | Longwave 1590 nm laser single-mode |
| CWDMSFP -1610 | Longwave 1610 nm laser single-mode |

Table 3 briefly describes the supported DWDM wavelengths on the Catalyst 4500-X Series Switches.

*Table 3 DWDM SFP Supported Wavelengths on the Cisco Catalyst 4500-X Series Switches*

| **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-5736= | Cisco 1000BASE-DWDM SFP 1557.36 nm |
| DWDM-SFP-5655= | Cisco 1000BASE-DWDM SFP 1556.55 nm |
| DWDM-SFP-5575= | Cisco 1000BASE-DWDM SFP 1555.75 nm |
| DWDM-SFP-5494= | Cisco 1000BASE-DWDM SFP 1554.94 nm |
| DWDM-SFP-5413= | Cisco 1000BASE-DWDM SFP 1554.13 nm |
| DWDM-SFP-5332= | Cisco 1000BASE-DWDM SFP 1553.33 nm |
| DWDM-SFP-5252= | Cisco 1000BASE-DWDM SFP 1552.52 nm |

*Table 3 DWDM SFP Supported Wavelengths on the Cisco Catalyst 4500-X Series Switches*

| **Product Number** (append with "=" for spares) | **Product Description** |
|---|---|
| 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-4931= | Cisco 1000BASE-DWDM SFP 1549.32 nm |
| DWDM-SFP-4851= | Cisco 1000BASE-DWDM SFP 1548.51 nm |
| DWDM-SFP-4772= | Cisco 1000BASE-DWDM SFP 1547.72 nm |
| DWDM-SFP-4694= | Cisco 1000BASE-DWDM SFP 1542.94 nm |
| DWDM-SFP-4692= | Cisco 1000BASE-DWDM SFP 1546.92 nm |
| DWDM-SFP-4614= | Cisco 1000BASE-DWDM SFP 1542.14 nm |
| DWDM-SFP-4612= | Cisco 1000BASE-DWDM SFP 1546.12 nm |
| DWDM-SFP-4532= | Cisco 1000BASE-DWDM SFP 1545.32 nm |
| DWDM-SFP-4453= | Cisco 1000BASE-DWDM SFP 1544.53 nm |
| DWDM-SFP-4373= | Cisco 1000BASE-DWDM SFP 1543.73 nm |
| DWDM-SFP-4134= | Cisco 1000BASE-DWDM SFP 1541.35 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-3739= | Cisco 1000BASE-DWDM SFP 1537.40 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-3346= | Cisco 1000BASE-DWDM SFP 1533.47 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 a complete list of Cisco Gigabit Ethernet Transceiver Modules, please refer to the URL:

http://www.cisco.com//c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6981.html#38544

Table 4 briefly describes the DOM support on the Catalyst 4500-X Series switches.

*Table 4 DOM Support on the Cisco Catalyst 4500-X Series Switches*

| | |
|---|---|
| SFP | GLC-BX-D |
| SFP | GLC-BX-U |
| SFP | GLC-LH-SMD |
| SFP | CWDM |
| SFP | DWDM (24 wavelengths) |
| SFP+ | SFP-10G-ER |
| SFP+ | SFP-10G-LR |
| SFP+ | SFP-10G-LRM |
| SFP+ | SFP-10G-SR |
| SFP+ | SFP-10G-ZR |

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

## Feature Support by Image Type

Table 5 is a detailed list of features supported on Catalyst 4500-X Series switches running Cisco IOS Software Release 3.5.0E categorized by image type. Please visit Feature Navigator for package details:

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

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| 2-way Community Private VLANs | Yes | Yes |
| 8-Way CEF Load Balancing | Yes | Yes |
| 10 Gigabit Uplink Use | Yes | Yes |
| AAA Server Group | Yes | Yes |
| AAA Server Group Based on DNIS | Yes | Yes |
| ACL - Improved Merging Algorithm | Yes | Yes |
| ACL Logging | Yes | Yes |
| ACL Policy Enhancements | Yes | Yes |
| ACL Sequence Numbering | Yes | Yes |
| Address Resolution Protocol (ARP) | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| ANCP Client | Yes | Yes |
| ANSI TIA-1057 LLDP - MED Location Extension | Yes | Yes |
| ANSI TIA-1057 LLDP - MED Support | Yes | Yes |
| ARP Optimization | Yes | Yes |
| Auto QoS | Yes | Yes |
| Auto SmartPorts | Yes | Yes |
| Auto-MDIX | Yes | Yes |
| Auto-Voice VLAN (part of Auto QoS) | Yes | Yes |
| AutoInstall Using DHCP for LAN Interfaces | Yes | Yes |
| AutoQoS - VoIP | Yes | Yes |
| AutoRP Enhancement | Yes | Yes |
| BGP | No | Yes |
| BGP 4 | No | Yes |
| BGP 4 4Byte ASN (CnH) | No | Yes |
| BGP 4 Multipath Support | No | Yes |
| BGP 4 Prefix Filter and In-bound Route Maps | No | Yes |
| BGP 4 Soft Config | No | Yes |
| BGP Conditional Route Injection | No | Yes |
| BGP Configuration Using Peer Templates | No | Yes |
| BGP Dynamic Update Peer-Groups | No | Yes |
| BGP Increased Support of Numbered as-path Access Lists to 500 | No | Yes |
| BGP Link Bandwidth | No | Yes |
| BGP Neighbor Policy | No | Yes |
| BGP Prefix-Based Outbound Route Filtering | No | Yes |
| BGP Restart Neighbor Session After max-prefix Limit Reached | No | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| BGP Route-Map Continue | No | Yes |
| BGP Route-Map Continue Support for Outbound Policy | No | Yes |
| BGP Soft Rest | No | Yes |
| BGP Wildcard | No | Yes |
| Bidirectional PIM (IPv4 only) | Yes | Yes |
| Boot Config | Yes | Yes |
| Broadcast/Multicast Suppression | Yes | Yes |
| Call Home | Yes | Yes |
| CDP (Cisco Discovery Protocol) Version 2 | Yes | Yes |
| CDP Enhancement - Host presence TLV | Yes | Yes |
| CEF/dCEF - Cisco Express Forwarding | Yes | Yes |
| CEFv6 Switching for 6to4 Tunnels | Yes | Yes |
| CEFv6/dCEFv6 - Cisco Express Forwarding | Yes | Yes |
| CFM/IEEE 802.1ag - D8.1 standard Compliant CFM, Y.1731 multicast LBM / AIS / RDI / LCK, IP SLA for Ethernet | Yes | Yes |
| CGMP - Cisco Group Management Protocol | Yes | Yes |
| Cisco IOS Scripting w/Tcl | Yes | Yes |
| Cisco Service Discovery Gateway Support | Yes | Yes |
| CiscoView Autonomous Device Manager (ADP) | Yes | Yes |
| Class Based Ethernet CoS Matching & Marking (802.1p & ISL CoS) | Yes | Yes |
| Class-Based Marking | Yes | Yes |
| Class-Based Policing | Yes | Yes |
| Class-Based Shaping | Yes | Yes |
| Clear Counters Per Port | Yes | Yes |
| CLI String Search | Yes | Yes |
| CNS | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| CNS - Configuration Agent | Yes | Yes |
| CNS - Event Agent | Yes | Yes |
| CNS - Image Agent | Yes | Yes |
| CNS - Interactive CLI | Yes | Yes |
| CNS Config Retrieve Enhancement with Retry and Interval | Yes | Yes |
| Command Scheduler (Kron) | Yes | Yes |
| Command Scheduler (Kron) Policy for System Startup | Yes | Yes |
| Commented IP Access List Entries | Yes | Yes |
| Community Private VLAN | Yes | Yes |
| Configuration Change Tracking Identifier | Yes | Yes |
| Configuration Change Notification and Logging | Yes | Yes |
| Configuration Replace and Configuration Rollback | Yes | Yes |
| Configuration Rollback Confirmed Change | Yes | Yes |
| Contextual Configuration Diff Utility | Yes | Yes |
| Control Plane Policing (Copp) | Yes | Yes |
| CPU Enhancement | Yes | Yes |
| CPU Optimization for Layer 3 Multicast Control Packets | Yes | Yes |
| Critical Authorization for Voice and Data | Yes | Yes |
| DAI (Dynamic ARP inspection) | Yes | Yes |
| DBL (Dynamic Buffer Limiting) - Selective DBL | Yes | Yes |
| Debounce Timer per Port | Yes | Yes |
| Default Passive Interface | Yes | Yes |
| DHCP Client | Yes | Yes |
| DHCP Configurable DHCP Client | Yes | Yes |
| DHCPv6 Relay Agent notification for Prefix Delegation | Yes | Yes |
| DHCP Option 82, Pass Through | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| DHCP Server | Yes | Yes |
| DHCP Snooping | Yes | Yes |
| DHCPv6 Ethernet Remote ID option | Yes | Yes |
| DHCPv6 Relay - Reload persistent Interface ID option | Yes | Yes |
| DHCPv6 Repackaging | Yes | Yes |
| Diffserv MIB | Yes | Yes |
| DSCP/CoS via LLDP | Yes | Yes |
| Duplication Location Reporting Issue | Yes | Yes |
| Dynamic Trunking Protocol (DTP) | Yes | Yes |
| Easy Virtual Network (EVN) | No | Yes |
| Embedded Event Manager | Yes | Yes |
| EIGRP | No | Yes |
| EIGRP Service Advertisement Framework | Yes | Yes |
| EIGRP Stub Routing | Yes | Yes |
| Embedded Event Manager (EEM) 3.2 | Yes | Yes |
| Embedded Syslog Manager (ESM) | Yes | Yes |
| Energywise Agentless SNMP support | Yes | Yes |
| Energywise Wake-On-Lan Support | Yes | Yes |
| Entity API for Physical and Logical Mgd Entities | Yes | Yes |
| ErrDisable timeout | Yes | Yes |
| EtherChannel | Yes | Yes |
| EtherChannel Flexible PAgP | Yes | Yes |
| EtherChannel Enhancement - Single Port Channel | Yes | Yes |
| Fast EtherChannel (FEC) | Yes | Yes |
| FHRP - Enhanced Object Tracking of IP SLAs | Yes | Yes |
| FHRP - EOT integration with EEM | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| FHRP - GLBP - IP Redundancy API | Yes | Yes |
| FHRP - HSRP - Hot Standby Router Protocol V2 | Yes | Yes |
| FHRP - Object Tracking List | Yes | Yes |
| Filter-ID Based ACL Application | Yes | Yes |
| FIPS 140-2/3 Level 2 Certification | Yes | Yes |
| Flexible NetFlow - Application ID | Yes | Yes |
| Flexible NetFlow - Device type | Yes | Yes |
| Flexible NetFlow - Ethertype | Yes | Yes |
| Flexible NetFlow - Export to an IPv6 address | Yes | Yes |
| Flexible NetFlow - Full Flow support | Yes | Yes |
| Flexible NetFlow - Ingress support | Yes | Yes |
| Flexible NetFlow - IPFIX | Yes | Yes |
| Flexible NetFlow - IPv4 Unicast Flows | Yes | Yes |
| Flexible NetFlow - IPv6 Unicast Flows | Yes | Yes |
| Flexible NetFlow - Layer 2 Fields | Yes | Yes |
| Flexible NetFlow - Multiple User Defined Caches | Yes | Yes |
| Flexible NetFlow - NetFlow Export over IPv4 | Yes | Yes |
| Flexible NetFlow - NetFlowV5 Export protocol | Yes | Yes |
| Flexible NetFlow - NetFlow v9 Export Format | Yes | Yes |
| Flexible NetFlow - Power Reading | Yes | Yes |
| Flexible NetFlow - Username | Yes | Yes |
| Flexible NetFlow - VLAN ID support | Yes | Yes |
| Flex Links+(VLAN Load balancing) | Yes | Yes |
| Embedded Event Manager (EEM) 3.2 | Yes | Yes |
| Forced 10/100 Autonegotiation | Yes | Yes |
| FTP Support for Downloading Software Images | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| Gateway Load Balancing Protocol GLBP | Yes | Yes |
| Generic Routing Encapsulation (GRE) | Yes | Yes |
| GOLD Online Diagnostics | Yes | Yes |
| HSRP - Hot Standby Router Protocol | Yes | Yes |
| HSRPv2 for IPv6 Global Address Support | Yes | Yes |
| HTTP Security | Yes | Yes |
| HTTP TACAC+ Accounting support | Yes | Yes |
| Identity 4.1 Network Edge Access Topology | Yes | Yes |
| IEEE 802.1ab LLDP (Link Layer Discovery Protocol) | Yes | Yes |
| IEEE 802.1ab LLDP/LLDP-MED | Yes | Yes |
| IEEE 802.1p Support | Yes | Yes |
| IEEE 802.1Q VLAN Trunking | Yes | Yes |
| IEEE 802.1s Multiple Spanning Tree (MST) Standard Compliance | Yes | Yes |
| IEEE 802.1s VLAN Multiple Spanning Trees | Yes | Yes |
| IEEE 802.1t[1] | Yes | Yes |
| IEEE 802.1w Spanning Tree Rapid Reconfiguration | Yes | Yes |
| IEEE 802.1x Auth Fail Open (Critical Ports) | Yes | Yes |
| IEEE 802.1x Auth Fail VLAN | Yes | Yes |
| IEEE 802.1x Flexible Authentication | Yes | Yes |
| IEEE 802.1x Multiple Authentication | Yes | Yes |
| IEEE 802.1x Open Authentication | Yes | Yes |
| IEEE 802.1x with User Distribution | Yes | Yes |
| IEEE 802.1x VLAN Assignment | Yes | Yes |
| IEEE 802.1x VLAN User Group Distribution | Yes | Yes |
| IEEE 802.1x Wake on LAN Support | Yes | Yes |
| IEEE 802.1x Authenticator | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| IEEE 802.1x Fallback support | Yes | Yes |
| IEEE 802.1x Guest VLAN | Yes | Yes |
| IEEE 802.1x Multi-Domain Authentication | Yes | Yes |
| IEEE 802.1x Private Guest VLAN | Yes | Yes |
| IEEE 802.1x Private VLAN Assignment | Yes | Yes |
| IEEE 802.1x RADIUS Accounting | Yes | Yes |
| IEEE 802.1x RADIUS-Supplied Session Timeout | Yes | Yes |
| IEEE 802.1x with ACL Assignments | Yes | Yes |
| IEEE 802.1x with Port Security | Yes | Yes |
| IEEE 802.3ad Link Aggregation (LACP) | Yes | Yes |
| IEEE 802.3ad Link Aggregation (LACP) Port-Channel Standalone Disable | Yes | Yes |
| IEEE 802.3x Flow Control | Yes | Yes |
| IGMP Fast Leave | Yes | Yes |
| IGMP Filtering | Yes | Yes |
| IGMP Snooping | Yes | Yes |
| IGMP Version 1 | Yes | Yes |
| IGMP Version 2 | Yes | Yes |
| IGMP Version 3 | Yes | Yes |
| IGMP Version 3 - Explicit Tracking of Hosts, Groups, and Channels | Yes | Yes |
| IGMPv3 Host Stack | Yes | Yes |
| IGMP Version 3 Snooping: Full Support | Yes | Yes |
| Image Verification | Yes | Yes |
| Individual SNMP Trap Support | Yes | Yes |
| Interface Index Persistence | Yes | Yes |
| Interface Range Specification | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

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

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| IP SLAs - UDP Jitter Operation | Yes | Yes |
| IP SLAs Video Operations | Yes | Yes |
| IP SLAs - VoIP Threshold Traps | Yes | Yes |
| IP Summary Address for RIPv2 | Yes | Yes |
| IP Unnumbered for VLAN-SVI interfaces | Yes | Yes |
| IPSG (IP Source Guard) v4 | Yes | Yes |
| IPSG (IP Source Guard) v4 for Static Hosts | Yes | Yes |
| IPv4 Policy Based Routing (PBR) | No | Yes |
| IPv4 Policy-Based Routing (PBR) Recursive Next Hop | No | Yes |
| IPv4 Routing: Static Hosts/Default Gateway | Yes | Yes |
| IPv6 (Internet Protocol Version 6) | Yes | Yes |
| IPv6 Access Services: DHCPv6 Relay Agent | Yes | Yes |
| IPv6 Anycast Address | Yes | Yes |
| IPv6 / v4 BFD with OSPF/ BGP/ EIGRP and Static | Yes | Yes |
| IPv6 BGP | No | Yes |
| IPv6 Bootstrap Router (BSR) Scoped Zone Support | No | Yes |
| IPv6 CNS Agents | Yes | Yes |
| IPv6 Config Logger | Yes | Yes |
| IPv6 First Hop Security (FHS):<br>DHCPv6 Guard<br>IPv6 Destination Guard<br>IPv6 Snooping (Data Gleaning, per-limit Address Limit)<br>IPv6 Neighbor Discovery Multicast Suppression<br>IPv6 Router Advertisement (RA) Guard | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| IPv6 First Hop Security (FHS) Phase 2:<br>Binding table recovery<br>Lightweight DHCPv6 Relay Agent (LDRA)<br>Neighbor Discovery (ND) Multicast Suppress<br>Source and Prefix Guard[2] | Yes | Yes |
| IPv6 HSRP | Yes | Yes |
| IPv6 HTTP(S) | Yes | Yes |
| IPv6 ICMPv6 | Yes | Yes |
| IPv6 ICMPv6 Redirect | Yes[3] | Yes |
| IPv6 IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect) | Yes | Yes |
| IPv6 Interface Statistics | Yes | Yes |
| IPv6 MLD Snooping v1 and v2 | Yes | Yes |
| IPv6 MTU Path Discovery | Yes | Yes |
| IPv6 Multicast | Yes | Yes |
| IPv6 Multicast: Bootstrap Router (BSR) | No | Yes |
| IPv6 Multicast: Explicit Tracking of Receivers | Yes | Yes |
| IPv6 Multicast: MLD Access Group | Yes | Yes |
| IPv6 Multicast: Multicast Listener Discovery (MLD) Protocol, Versions 1 and 2 | Yes | Yes |
| IPv6 Multicast: PIM Accept Register | Yes | Yes |
| IPv6 Multicast: PIM Embedded RP Support | Yes | Yes |
| IPv6 Multicast: PIM Source-Specific Multicast (PIM-SSM) | Yes | Yes |
| IPv6 Multicast: PIM Sparse Mode (PIM-SM) | Yes | Yes |
| IPv6 Multicast: Routable Address Hello Option | Yes | Yes |
| IPv6 Multicast: RPF Flooding of Bootstrap Router (BSR) Packets | Yes | Yes |
| IPv6 Multicast: Scope Boundaries | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| IPv6 Neighbor Discovery | Yes | Yes |
| IPv6 Neighbor Discovery Duplicate Address Detection | Yes | Yes |
| IPv6 OSPFv3 NSF/SSO | Yes[3] | Yes |
| IPv6 OSPFv3 Fast Convergence | Yes | Yes |
| IPv6 RA Guard (Host Mode) | Yes | Yes |
| IPv6 Routing - EIGRP Support | No | Yes |
| IPv6 Routing: OSPF for IPv6 (OSPFv3) | Yes[3] | Yes |
| IPv6 Routing: RIP for IPv6 (RIPng) | Yes | Yes |
| IPv6 Routing: Route Redistribution | Yes | Yes |
| IPv6 Routing: Static Routing | Yes | Yes |
| IPv6 Security: Secure Shell SSH support over IPv6 | Yes | Yes |
| IPv6 Services: AAAA DNS Lookups over an IPv4 Transport | Yes | Yes |
| IPv6 Services: Cisco Discovery Protocol (CDP) - IPv6 Address Family Support for Neighbor Information | Yes | Yes |
| IPv6 Services: DNS Lookups over an IPv6 Transport | Yes | Yes |
| IPv6 Services: Extended Access Control Lists | Yes | Yes |
| IPv6 Services: Standard Access Control Lists | Yes | Yes |
| IPv6 Stateless Auto-configuration | Yes | Yes |
| IPv6 Switching: CEF Support | Yes | Yes |
| IPv6 Switching: CEFv6 Switched Automatic IPv4-compatible Tunnels (in software) | Yes | Yes |
| IPv6 Switching: CEFv6 Switched Configured IPv6 over IPv4 Tunnels (in software) | Yes | Yes |
| IPv6 Switching: CEFv6 Switched ISATAP Tunnels (in software) | Yes | Yes |
| IPv6 TCL | Yes | Yes |
| IPv6 Tunneling: Automatic 6to4 Tunnels (in software) | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| IPv6 Tunneling: Automatic IPv4-compatible Tunnels (in software) | Yes | Yes |
| IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels (in software) | Yes | Yes |
| IPv6 Tunneling: ISATAP Tunnel Support (in software) | Yes | Yes |
| IPv6 Tunneling: Manually Configured IPv6 over IPv4 Tunnels (in software) | Yes | Yes |
| IPv6 Virtual LAN Access Control List (VACL) | Yes | Yes |
| IPsecv3/IKEv2 (for management traffic only) | Yes | Yes |
| IS-IS for IPv4 and IPv6 | No | Yes |
| ISSU (IOS In-Service Software Upgrade) | Yes | Yes |
| Jumbo Frames | Yes | Yes |
| Layer 2 Control Packet | Yes | Yes |
| Layer 2 Protocol Tunneling (L2PT) | Yes | Yes |
| Layer 2 Traceroute | Yes | Yes |
| Layer 3 Multicast Routing (PIM SM, SSM, Bidir) | Yes | Yes |
| Link State Tracking | Yes | Yes |
| Loadsharing IP packets over more than six parallel paths | Yes | Yes |
| Local Proxy ARP | Yes | Yes |
| Location MIBs | Yes | Yes |
| MAB for Voice VLAN | Yes | Yes |
| MAB with Configurable User Name/Password | Yes | Yes |
| MAC Address Notification | Yes | Yes |
| MAC Authentication Bypass | Yes | Yes |
| MAC Move and Replace | Yes | Yes |
| Medianet 2.0: AutoQoS SRND4 Macro | Yes | Yes |
| Medianet 2.0: Integrated Video Traffic Simulator (hardware-assisted IP SLA); IPSLA generator and responder | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| Medianet 2.0: Flow Metadata | Yes | Yes |
| Medianet 2.0: Media Service Proxy | Yes | Yes |
| Medianet 2.0: Media Monitoring (Performance Monitoring and Mediatrace) | Yes | Yes |
| Memory Threshold Notifications | Yes | Yes |
| Microflow policers | Yes | Yes |
| Modular QoS CLI (MQC) | Yes | Yes |
| Multi-authentication and VLAN Assignment | Yes | Yes |
| Multi-VRF Support (VRF lite) | No | Yes |
| Multicast BGP (MBGP) | No | Yes |
| Multicast Fast Switching Performance Improvement | Yes | Yes |
| Multicast Routing Monitor (MRM) | Yes | Yes |
| Multicast Source Discovery Protocol (MSDP) | Yes | Yes |
| Multicast Subsecond Convergence | Yes | Yes |
| Multicast VLAN Registration (MVR) | Yes | Yes |
| NAC - L2 IEEE 802.1x | Yes | Yes |
| NAC - L2 IP | Yes | Yes |
| ND Cache Limit/Interface | Yes | Yes |
| NETCONF over SSHv2 | Yes | Yes |
| Network Edge Access Topology (NEAT) | Yes | Yes |
| NEAT Enhancement: Re-Enabling BPDU Guard Based on User Configuration | Yes | Yes |
| Network Time Protocol (NTP) | Yes | Yes |
| Network Time Protocol (NTP) master | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| NMSP Enhancements<br>• GPS support for location<br>• Location at switch level<br>• Local timezone change<br>• Name value pair<br>• Priority settings for MIBs | Yes | Yes |
| No Service Password Recovery | Yes | Yes |
| No. of VLAN Support | 4096 | 4096 |
| NSF - BGP | No | Yes |
| NSF - EIGRP | Yes | Yes |
| NSF - OSPF (version 2 only) | Yes | Yes |
| NSF - SSO | Yes | Yes |
| NTP for IPv6 | Yes | Yes |
| NTP for VRF aware | No | Yes |
| Onboard Failure Logging (OBFL) | Yes | Yes |
| OSPF | Yes[3] | Yes |
| OSPF v3 Authentication | Yes[3] | Yes |
| OSPF Flooding Reduction | Yes[3] | Yes |
| OSPF for Routed Access[4] | Yes | Yes |
| OSPF Incremental Shortest Path First (i-SPF) Support | Yes[3] | Yes |
| OSPF Link State Database Overload Protection | Yes[3] | Yes |
| OSPF Not-So-Stubby Areas (NSSA) | Yes[3] | Yes |
| OSPF Packet Pacing | Yes[3] | Yes |
| OSPF Shortest Paths First Throttling | Yes[3] | Yes |
| OSPF Stub Router Advertisement | Yes[3] | Yes |
| OSPF Support for Fast Hellos | Yes[3] | Yes |
| OSPF Support for Link State Advertisement (LSA) Throttling | Yes[3] | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| OSPF Support for Multi-VRF on CE Routers | Yes[3] | Yes |
| OSPF Update Packet-Pacing Configurable Timers | Yes[3] | Yes |
| Out-of-band Management Port | Yes | Yes |
| Out-of-band Management Port - IPv6 | Yes | Yes |
| Per Intf IGMP State Limit | Yes | Yes |
| Per Intf MrouteState Limit | Yes | Yes |
| Per Port Per VLAN Policing | Yes | Yes |
| Per-User ACL Support for 802.1X/MAB/Webauth users | Yes | Yes |
| Per-VLAN Learning | Yes | Yes |
| Permanent Right-to-Use (PRTU) license | Yes | Yes |
| PIM Dense Mode State Refresh | Yes | Yes |
| PIM Multicast Scalability | Yes | Yes |
| PIM Version 1 | Yes | Yes |
| PIM Version 2 | Yes | Yes |
| Port Security | Yes (supports 3072 MACs) | Yes (supports 3072 MACs) |
| Port Security on Etherchannel Trunk Port | Yes | Yes |
| Pragmatic General Multicast (PGM) | Yes | Yes |
| Priority Queueing (PQ) | Yes | Yes |
| Private VLAN Promiscuous Trunk Port | Yes | Yes |
| Private VLAN Trunk Ports | Yes | Yes |
| Private VLANs | Yes | Yes |
| Propagation of Location Info over CDP | Yes | Yes |
| PVLAN over EtherChannel | Yes | Yes |
| PVST + (Per VLAN Spanning Tree Plus) | Yes | Yes |
| Q-in-Q | Yes | Yes |
| QoS Packet Marking | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| QoS Priority Percentage CLI Support | Yes | Yes |
| RADIUS | Yes | Yes |
| RADIUS Attribute 44 (Accounting Session ID) in Access Requests | Yes | Yes |
| RADIUS Change of Authorization | Yes | Yes |
| Rapid PVST+ Dispute Mechanism | Yes | Yes |
| Rapid-Per-VLAN-Spanning Tree (Rapid-PVST) | Yes | Yes |
| Reduced MAC Address Usage | Yes | Yes |
| Redundancy Facility Protocol | Yes | Yes |
| Remote SPAN (RSPAN) | Yes | Yes |
| REP (Resilient Ethernet Protocol) | Yes | Yes |
| REP - No Edge Neighbour Enhancement | Yes | Yes |
| RIP v1 | Yes | Yes |
| RMON events and alarms | Yes | Yes |
| Secure Copy (SCP) | Yes | Yes |
| Secure Shell SSH Version 1 Integrated Client | Yes | Yes |
| Secure Shell SSH Version 1 Server Support | Yes | Yes |
| Secure Shell SSH Version 2 Client Support | Yes | Yes |
| Secure Shell SSH Version 2 Server Support | Yes | Yes |
| Single Rate 3-Color Marker for Traffic Policing | Yes | Yes |
| Smart Install Director—Configuration-only Deployment and Smooth Upgrade | Yes | Yes |
| Smart Port | Yes | Yes |
| SNMP (Simple Network Management Protocol) | Yes | Yes |
| SNMP Inform Request | Yes | Yes |
| SNMP Manager | Yes | Yes |
| SNMPv2C | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| SNMPv3 - 3DES and AES Encryption Support | Yes | Yes |
| SNMPv3 (SNMP Version 3) | Yes | Yes |
| Source Specific Multicast (SSM) | Yes | Yes |
| Source Specific Multicast (SSM) - IGMPv3,IGMP v3lite, and URD | Yes | Yes |
| Source Specific Multicast (SSM) Mapping | Yes | Yes |
| SPAN (# of sessions) – Port Mirroring | Yes (16 bidirectional sessions) | Yes (16 bidirectional sessions) |
| SPAN ACL Filtering for IPv6 | Yes | Yes |
| Span Enhancement: Packet Type and Address Type Filtering | Yes | Yes |
| Spanning Tree Protocol (STP) | Yes | Yes |
| Spanning Tree Protocol (STP) - Backbone Fast Convergence | Yes | Yes |
| Spanning Tree Protocol (STP) - Loop Guard | Yes | Yes |
| Spanning Tree Protocol (STP) - Portfast | Yes | Yes |
| Spanning Tree Protocol (STP) - PortFast BPDU Filtering | Yes | Yes |
| Spanning Tree Protocol (STP) - Portfast BPDU Guard | Yes | Yes |
| Spanning Tree Protocol (STP) - Portfast Support for Trunks | Yes | Yes |
| Spanning Tree Protocol (STP) - Root Guard | Yes | Yes |
| Spanning Tree Protocol (STP) - Uplink Fast Convergence | Yes | Yes |
| Spanning Tree Protocol (STP) - Uplink Load Balancing | Yes | Yes |
| Spanning Tree Protocol (STP) Extension | Yes | Yes |
| Standard IP Access List Logging | Yes | Yes |
| Standby Supervisor Port Usage | Yes | Yes |
| Sticky Port Security | Yes | Yes |
| Sticky Port Security on Voice VLAN | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| Storm Control - Per-Port Multicast Suppression | Yes | Yes |
| STP Syslog Messages | Yes | Yes |
| Stub IP Multicast Routing | Yes | Yes |
| Sub-second UDLD | Yes | Yes |
| SVI (Switch Virtual Interface) Autostate Exclude | Yes | Yes |
| Switch and IP Phone Security Interaction | Yes | Yes |
| Switch Port Analyzer (SPAN) | Yes | Yes |
| Switch Port Analyzer (SPAN) - CPU Source | Yes | Yes |
| Syslog over IPV6 | Yes | Yes |
| System Logging - EAL4 Certification Enhancements | Yes | Yes |
| TACACS SENDAUTH function | Yes | Yes |
| TACACS Single Connection | Yes | Yes |
| TACACS+ | Yes | Yes |
| TACACS+ and Radius for IPv6- | Yes | Yes |
| TCAM4 - Dynamic Multi-Protocol | Yes | Yes |
| TCAM4 - Service-Aware Resource Allocation | Yes | Yes |
| Time Domain Reflectometry (TDR) | Yes | Yes |
| Time-Based Access Lists | Yes | Yes |
| Time-Based Access Lists Using Time Ranges (ACL) | Yes | Yes |
| Trusted boundary (extended trust for CDP devices) | Yes | Yes |
| TrustSec: IEEE 802.1ae MACSec Layer 2 encryption | Yes | Yes |
| TrustSec: IEEE 802.1ae MACSec encryption on user facing ports | Yes | Yes |
| TrustSec: IEEE 802.1ae MACSec encryption between switch-to-switch links using Cisco SAP (Security Association Protocol) | Yes | Yes |
| TrustSec SGT Exchange Protocol (SXP) IPv4 | Yes | Yes |
| TrustSec SGT/ SGA | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| UDI - Unique Device Identifier | Yes | Yes |
| Uni-Directional Link Routing (UDLR) | Yes | Yes |
| Unicast Mac Filtering | Yes | Yes |
| Unicast Reverse Path Forwarding (uRPF) | Yes | Yes |
| Unidirectional Ethernet | Yes | Yes |
| UniDirectional Link Detection (UDLD) | Yes | Yes |
| Virtual Router Redundancy Protocol (VRRP) for IPv4 | Yes | Yes |
| Virtual Switching System (VSS) | Yes | Yes |
| Virtual Switching System (VSS) Phase 2[5]<br>• Support for Layer 3 MEC—VSS with Layer 3 Multichassis EtherChannel (MEC) at the aggregation layer<br>• 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.<br>• Support for VSL Encryption | Yes | Yes |
| Virtual Trunking Protocol (VTP) - Pruning | Yes | Yes |
| VLAN Access Control List (VACL) | Yes | Yes |
| VLAN MAC Address Filtering | Yes | Yes |
| VLAN Mapping (VLAN Translation) | Yes | Yes |
| VRF-aware TACACS+ | No | Yes |
| VRF-lite for IPv6 on OSPF/ BGP/ EIGRP | No | Yes |
| VTP (Virtual Trunking Protocol) Version 2 | Yes | Yes |
| VTP Version 3 | Yes | Yes |
| WCCP Version 2 | Yes | Yes |
| Web Authentication Proxy | Yes | Yes |
| Webauth Enhancements | Yes | Yes |
| Wireshark-based Ethernet Analyzer | Yes | Yes |

*Table 5 IP Base and Enterprise Services Image Support on Cisco Catalyst 4500-X Series*

| Feature | IP Base | Enterprise Services |
|---|---|---|
| XML-PI | 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 1000 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. As of IOS Release 3.5.0E, 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 4500-X Series Switches

The following features are not supported on a Catalyst 4500-X Series switches:

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

With some exceptions, the VSS maintains “feature parity” with the standalone Catalyst 4500 or 4500-X series switches. Major exceptions include:

- CFM D8.1
- Dot1q Tunnel (**“legacy/classic”** dot1q tunnel)
- Dot1q tunneling and L2PT (Layer 2 Protocol Tunneling)
- Fast UDLD
- Flexlink
- Mediatrace (Medianet active video monitoring feature)
- Metadata (Medianet feature)
- Per VLAN Learning
- REP and associated featurettes
- UDE
- UDLR
- VLAN Translation (1:1 and 1:2-Selective QinQ)
- VMPS Client

- WCCP

## Orderable Product Numbers

*Table 6 Cisco IOS XE Software Release 3.5.0E Product Numbers and Images for the Catalyst 4500-X Series Switches*

| Product Number | Description | Image |
|---|---|---|
| **Base Switch PIDs** | | |
| WS-C4500X-32SFP+ | Catalyst 4500-X 32 Port 10GE IP Base, Front-to-Back Cooling i.e. Port Side to Power Supply Cooling with no Power Supply | cat4500e-universal.SPA.03.04.00.SG.151-2.SG.bin<br>cat4500e-universalk9.SPA.03.04.00.SG.151-2.SG.bin |
| WS-C4500X-F-32SFP+ | Catalyst 4500-X 32 Port 10GE IP Base, Back-to-Front Cooling i.e. Power Supply to Port Side Cooling with no Power Supply | cat4500e-universal.SPA.03.04.00.SG.151-2.SG.bin<br>cat4500e-universalk9.SPA.03.04.00.SG.151-2.SG.bin |
| WS-C4500X-16SFP+ | Catalyst 4500-X 16 Port 10GE IP Base, Front-to-Back Cooling i.e. Port Side to Power Supply Cooling with no Power Supply | cat4500e-universal.SPA.03.04.00.SG.151-2.SG.bin<br>cat4500e-universalk9.SPA.03.04.00.SG.151-2.SG.bin |
| WS-C4500X-F-16SFP+ | Catalyst 4500-X 16 Port 10GE IP Base, Back-to-Front Cooling i.e. Power Supply to Port Side Cooling with no Power Supply | cat4500e-universal.SPA.03.04.00.SG.151-2.SG.bin<br>cat4500e-universalk9.SPA.03.04.00.SG.151-2.SG.bin |
| WS-C4500X-24X-IPB | Catalyst 4500-X 24 Port 10GE IP Base, Front-to-Back Cooling (Power Supplies must be configured) | cat4500e-universal.SPA.03.04.00.SG.151-2.SG.bin<br>cat4500e-universalk9.SPA.03.04.00.SG.151-2.SG.bin |
| WS-C4500X-40X-ES | Catalyst 4500-X 40 Port 10G Enterprise Services, Front-to-Back Cooling, No Power Supply | cat4500e-universal.SPA.03.04.00.SG.151-2.SG.bin<br>cat4500e-universalk9.SPA.03.04.00.SG.151-2.SG.bin |
| WS-C4500X-24X-ES | Catalyst 4500-X 24 Port 10G Enterprise Services, Front-to-Back Cooling, No Power Supply | cat4500e-universal.SPA.03.04.00.SG.151-2.SG.bin<br>cat4500e-universalk9.SPA.03.04.00.SG.151-2.SG.bin |
| **FRU and OIR FANs** | | |
| C4KX-FAN-F | Catalyst 4500-X Back-to-Front Cooling Fan | NA |
| C4KX-FAN-R | Catalyst 4500-X Front-to-Back Cooling Fan | NA |

*Table 6 Cisco IOS XE Software Release 3.5.0E Product Numbers and Images for the Catalyst 4500-X Series Switches*

| Product Number | Description | Image |
|---|---|---|
| **Power Supply** | | |
| C4KX-PWR-750AC-F | Catalyst 4500-X 750W AC Back-to-Front Cooling Power Supply (primary) | N/A |
| C4KX-PWR-750AC-F/2 | Catalyst 4500-X 750W AC Back-to-Front Cooling Power Supply (secondary) | N/A |
| C4KX-PWR-750AC-R | Catalyst 4500-X 750W AC Front-to-Back Cooling Power Supply (primary) | N/A |
| C4KX-PWR-750AC-R/2 | Catalyst 4500-X 750W AC Front-to-Back Cooling Power Supply (secondary) | N/A |
| C4KX-PWR-750DC-F | Catalyst 4500-X 750W DC Back-to-Front Cooling Power Supply (primary) | N/A |
| C4KX-PWR-750DC-F/2 | Catalyst 4500-X 750W DC Back-to-Front Cooling Power Supply (secondary) | N/A |
| C4KX-PWR-750DC-R | Catalyst 4500-X 750W DC Front-to-Back Cooling Power Supply (primary) | N/A |
| C4KX-PWR-750DC-R/2 | Catalyst 4500-X 750W DC Front-to-Back Cooling Power Supply (secondary) | N/A |
| **Accessories** | | |
| CAB-CON-C4K-RJ45 | Console Cable 6ft with RJ-45-to-RJ-45 | N/A |
| SD-X45-2GB-E | Cisco Catalyst 4500 2-GB SD card | N/A |
| USB-X45-4GB-E | Cisco Catalyst 4500 4-GB USB device | N/A |
| C4KX-NM-8SFP+ | Catalyst 4500-X 8 Port 10GE Network Module | N/A |
| **Software** | | |
| S45XU-35-1521E | CAT4500-X Universal Image | cat4500e-universal.SPA.03.05.00.E.152-1E.bin |

*Table 6 Cisco IOS XE Software Release 3.5.0E Product Numbers and Images for the Catalyst 4500-X Series Switches*

| Product Number | Description | Image |
|---|---|---|
| S45XUK9-35-1521E | CAT4500-X Universal Crypto image | cat4500e-universalk9.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-X Series switch running Cisco IOS XE software:

- New Hardware Features in Release IOS XE 3.5.0E, page 29
- New Software Features in Release IOS XE 3.5.0E, page 29

## New Hardware Features in Release IOS XE 3.5.0E

- SFP+DWDM

## 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)

C3PL DSMIB

Common Criteria

Configurable TCP Keep Alive Timer.

DCM 2.0

DHCP Glean

DHCPv6 Relay Chaining and Route Insertion

Diffserv MIB (RFC 3289) support

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 PBR for 4k in IP Base Package

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 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
- 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

Manually Configured Tunnel over IPv4

Multicast VLAN Registration (MVR)

Layer 3 Multichassis Ethernet Channel

Legacy Line Cards Support in VSS system

MACSec Encryption on Cisco Catalyst 4500-X

- IEEE 802.1ae MACSec Layer 2 encryption
- IEEE 802.1ae MACSec encryption on user-facing ports
- IEEE 802.1ae MACSec encryption between switch-to-switch links using Cisco Security Association Protocol (SAP)

Manually Configured Tunnel over IPv4

mDNS Bonjour Support

MIB Gaps

- CISCO-EMBEDDED-EVENT-MGR-MIB
- SNMP-COMMUNITY-MIB

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

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

## 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.

**New Features:**

**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/config-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-non-contiguous-ports.html

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

### \OSPFv3 Max-Metric Router-Lsa

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-e/ip6-route-ospfv3-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_chapter_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 |
|---|---|
| 03.3.0SG | 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 IOS XE Version 3.5.0E and are planning on using VSS, you must upgrade your ROMMON to IOS Version 15.0(1r)SG10. Else, leave the ROMMON at its default level.

# Limitations and Restrictions

- Starting with Release IOS XE 3.3.0SG, the seven RP restriction was removed.
- 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 (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 an 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
- When OSPFv3 LSA throttling is configured, rate limiting does not take effect for a few minutes.

  **WorkAround**: None. CSCtw86319
- The ROMMON version number column in the output of **show module** command is truncated.

  **Workaround**: Use the **show version** command. CSCtr30294
- IP SLA session creation fails randomly for various 4-tuples.

  **Workaround**: Select an alternate destination or source port. CSCty05405
- The system cannot scale to greater than 512 SIP flows with MSP and metadata enabled.

  **Workaround**: None. CSCty79236
- When 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

- An incorrect module number is displayed in the console messages during boot up of a Cat4500X VSS.

  ```
  *Jul 18 12:36:11.138: %C4K_IOSMODPORTMAN-6-MODULEONLINE: Module 11 (WS-C4500X-32
   S/N: JAE154503I8 Hw: 1.0) is online
  ```

  Because the Catalyst 4500-X is a “fixed” configuration device, in a VSS, you would expect the two systems to be labeled 'Module 1' and 'Module 2.' However, because of software implementation similarities with the modular Catalyst 4500E series switches, the Standby switch is labeled 'Module 11.'

  **Workaround**: None. CSCub11632

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

  **Workaround**: None. CSCuc77376

- 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 display flow statistics.

  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

- When MLD Snooping is disabled, a Catalyst 4500-X switch cannot maintain 6,000 MLD joins, causing traffic loss due to missing outgoing interfaces.

  **Workaround**: Enable MLD snooping. CSCtx82176

- When a Catalyst 4500-X uplink module is removed incorrectly, hardware forwarding tables are frozen, and baseboard ports remain connected for 20 to 25 seconds.

  **Workaround**: Remove the Catalyst 4500-X module by first pressing the **Ejector** button for 10 seconds until the light turns green. CSCty67871

  **Caution**: If you remove the module without following this procedure, the system always shuts down (or fails). Always use the **Ejector** button.

- For the 10-Gigabit interface on a Catalyst 4500-X switch, link flaps are observed if the debounce interval is defined with the **link debounce time** command to within 1 second of the pulse interval.

  For example, if the pulse interval is 250 ms and the debounce interval is 500 ms, then the delta is 250 ms and the debounce will be ineffective.

  **Workaround**: Define a debounce interval that is at least 1 second greater than the incoming pulse interval. CSCtx75188

- 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 with 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...Predator and K10
- 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
- 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

- 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
- 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
- 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
- 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

- While performing an ISSU upgrade from a prior release (like upgrading IOS Release XE 3.3.0SG (or 3.4.0SG) to 3.5.0E) 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 behavior does not impact functionality.

  **Workaround**: None. CSCuh47387

- 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

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

  **Workaround**: None  CSCug79180

- UDE does not function at 1Gbps.

  **Workaround**: None. CSCuj56314

- 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 3.5.3E

- None

## 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 display flow statistics.

  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

- When MLD Snooping is disabled, a Catalyst 4500-X switch cannot maintain 6,000 MLD joins, causing traffic loss due to missing outgoing interfaces.

  **Workaround**: Enable MLD snooping. CSCtx82176

- When a Catalyst 4500-X uplink module is removed incorrectly, hardware forwarding tables are frozen, and baseboard ports remain connected for 20 to 25 seconds.

  **Workaround**: Remove the Catalyst 4500-X module by first pressing the **Ejector** button for 10 seconds until the light turns green. CSCty67871

  **Caution**: If you remove the module without following this procedure, the system always shuts down (or fails). Always use the **Ejector** button.

- For the 10-Gigabit interface on a Catalyst 4500-X switch, link flaps are observed if the debounce interval is defined with the **link debounce time** command to within 1 second of the pulse interval.

  For example, if the pulse interval is 250 ms and the debounce interval is 500 ms, then the delta is 250 ms and the debounce will be ineffective.

  **Workaround**: Define a debounce interval that is at least 1 second greater than the incoming pulse interval. CSCtx75188
- 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 with 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...Predator and K10

- 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

- 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

- 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

- 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

- 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

- 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

- While performing an ISSU upgrade from a prior release (like upgrading IOS Release XE 3.3.0SG (or 3.4.0SG) to 3.5.0E) 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 behavior does not impact functionality.

  **Workaround**: None. CSCuh47387

- 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

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

  **Workaround**: None  CSCug79180

- UDE does not function at 1Gbps.

  **Workaround**: None. CSCuj56314
- 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 display flow statistics.

  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

- When MLD Snooping is disabled, a Catalyst 4500-X switch cannot maintain 6,000 MLD joins, causing traffic loss due to missing outgoing interfaces.

  **Workaround**: Enable MLD snooping. CSCtx82176

- When a Catalyst 4500-X uplink module is removed incorrectly, hardware forwarding tables are frozen, and baseboard ports remain connected for 20 to 25 seconds.

  **Workaround**: Remove the Catalyst 4500-X module by first pressing the **Ejector** button for 10 seconds until the light turns green. CSCty67871

  **Caution**: If you remove the module without following this procedure, the system always shuts down (or fails). Always use the **Ejector** button.

- For the 10-Gigabit interface on a Catalyst 4500-X switch, link flaps are observed if the debounce interval is defined with the **link debounce time** command to within 1 second of the pulse interval.

  For example, if the pulse interval is 250 ms and the debounce interval is 500 ms, then the delta is 250 ms and the debounce will be ineffective.

  **Workaround**: Define a debounce interval that is at least 1 second greater than the incoming pulse interval. CSCtx75188

- 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 with 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...Predator and K10
- 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
- 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
- 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
- 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

- 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

- 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

- While performing an ISSU upgrade from a prior release (like upgrading IOS Release XE 3.3.0SG (or 3.4.0SG) to 3.5.0E) 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 behavior does not impact functionality.

  **Workaround**: None. CSCuh47387

- 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

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

  **Workaround**: None  CSCug79180

- UDE does not function at 1Gbps.

  **Workaround**: None. CSCuj56314

- 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

- A Catalyst 4500-X switch might crash while running the Wireshark feature provided you do the following:

**Step 1** Start “capture” with an IPv4, IPv6, or MAC filter (using the **match** keyword).

**Step 2** Stop “capture and configure for a different filter.

**Step 3** Re-start “capture.”

  **Workaround**: Use an acl/class-map (in config mode) rather than the "**monitor capture** *name* **match** [**ipv4 | ipv6 | mac**] command. CSCuj23896

- 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

- 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 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

- 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

- 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

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

  **Workaround**: None. CSCul00025

## Open Caveats for Cisco IOS XE Release 3.5.0E

- 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 display flow statistics.

  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
- When MLD Snooping is disabled, a Catalyst 4500-X switch cannot maintain 6,000 MLD joins, causing traffic loss due to missing outgoing interfaces.

  **Workaround**: Enable MLD snooping. CSCtx82176
- When a Catalyst 4500-X uplink module is removed incorrectly, hardware forwarding tables are frozen, and baseboard ports remain connected for 20 to 25 seconds.

  **Workaround**: Remove the Catalyst 4500-X module by first pressing the **Ejector** button for 10 seconds until the light turns green. CSCty67871

  **Caution**: If you remove the module without following this procedure, the system always shuts down (or fails). Always use the **Ejector** button.
- For the 10-Gigabit interface on a Catalyst 4500-X switch, link flaps are observed if the debounce interval is defined with the **link debounce time** command to within 1 second of the pulse interval.

  For example, if the pulse interval is 250 ms and the debounce interval is 500 ms, then the delta is 250 ms and the debounce will be ineffective.

**Workaround**: Define a debounce interval that is at least 1 second greater than the incoming pulse interval. CSCtx75188

- 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 with 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...Predator and K10

- 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

- 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

- 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

- 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

- 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

- 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

- While performing an ISSU upgrade from a prior release (like upgrading IOS Release XE 3.3.0SG (or 3.4.0SG) to 3.5.0E) 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 behavior does not impact functionality.

  **Workaround**: None. CSCuh47387

- 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

- 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

- UDE does not function at 1Gbps.

  **Workaround**: None. CSCuj56314

- 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

- 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

- 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-X series information:

- Catalyst 4500-X Series Switch Documentation Home

  http://www.cisco.com//en/US/products/ps12332/index.html

## Hardware Documents

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

- *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
- Catalyst 4500-X hardware installation information is available at:

  http://www.cisco.com/en/US/products/ps12332/prod_installation_guides_list.html

## Software Documentation

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

- Cisco 4500-X release notes are available at:

  http://www.cisco.com/en/US/products/ps12332/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.

# Obtaining Documentation and Submitting a Service Request

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

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

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

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