Release Notes for the Catalyst 4500-X Series Switches, Cisco IOS XE Release 3.4.xSG

Current release
IOS XE 3.4.8 SG—Nov 11, 2016

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

This release note describes the features, modifications, and caveats for the Cisco IOS XE 3.4.xSG software on the Catalyst 4500-X Series switch

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

Cisco IOS XE Software Release 3.4.0SG delivers new software and hardware innovations in campus access and aggregation deployments that span across many technologies including Security, Video, HighAvailability, NetworkVirtualization, IPMulticast and Lower TCO as following:

High Availability

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

Security

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

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

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

Lower Total Cost of Ownership and Ease of Use

- Smart Install (Director Support)

Routing and Multicast Enhancements

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

IPv6 Access Control

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

Other

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

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

http://www.cisco.com/en/US/products/products_end-of-life_policy.html

For more information on the Catalyst 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:

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

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

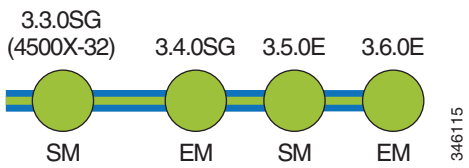
Cisco IOS XE Release Strategy

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

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 3.4.0SG follows the standard Cisco Systems® support policy, available at

http://www.cisco.com/en/US/products/products_end-of-life_policy.html

System Requirements

This section describes the system requirements:

Supported Hardware on the Catalyst 4500-X Series Switches

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

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

Table 1 lists the hardware supported on the Catalyst 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 For DOM support, see Table 4 on page 7.
GLC-BX-U	1000BASE-BX10-U small form-factor pluggable module For DOM support, see Table 4 on page 7.bv
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-EX-SMD	1000BASE-EX 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 5 for a list of supported wavelengths.) For DOM support, see Table 4 on page 7.

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

Product Number (append with "=" for spares)	**Product Description**
SFP+ Modules	
SFP-10G-SR	Cisco 10GBASE-SR SFP+ Module for MMF
SFP-10G-LR	Cisco 10GBASE-LR SFP+ Module for SMF
SFP-10G-LRM	Cisco 10GBASE-LRM SFP+ Module for MMF
SFP-H10GB-CU1M	10GBASE-CU SFP+ Cable 1 Meter
SFP-H10GB-CU3M	10GBASE-CU SFP+ Cable 3 Meter
SFP-H10GB-CU5M	10GBASE-CU SFP+ Cable 5 Meter
SFP-10G-ER	Cisco 10GBASE-ER SFP+ Module for SMF
SFP-10G-ZR	Cisco 10GBASE-ZR SFP+ Module for SMF **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-6141=	Cisco 1000BASE-DWDM SFP 1561.42 nm
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

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

Product Number (append with "=" for spares)	**Product Description**
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
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

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 3.4.0SG 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
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
CNS - Configuration Agent	Yes	Yes

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

Feature	IP Base	Enterprise Services
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
DHCP Server	Yes	Yes

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

Feature	IP Base	Enterprise Services
DHCP Snooping	Yes	Yes
DHCPv6 Ethernet Remote ID option	Yes	Yes
DHCPv6 Relay - Reload persistent Interface ID option	Yes	Yes
DHCPv6 Repackaging	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
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[1]	Yes	Yes
FHRP - EOT integration with EEM	Yes	Yes
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

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

Feature	IP Base	Enterprise Services
FIPS 140-2/3 Level 2 Certification	Yes	Yes
Flexible NetFlow - Full Flow support	Yes	Yes
Flexible NetFlow - Ingress support	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 - 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
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

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

Feature	IP Base	Enterprise Services
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[2]	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
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

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

Feature	IP Base	Enterprise Services
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
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

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

Feature	IP Base	Enterprise Services
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
IP SLAs - UDP Jitter Operation	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 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

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

Feature	IP Base	Enterprise Services
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): DHCPv6 Guard Lightweight DHCPv6 Relay Agent IPv6 Destination Guard IPv6 Snooping IPv6 Neighbor Discovery Multicast Suppression IPv6 Router Advertisement (RA) Guard	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

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

Feature	IP Base	Enterprise Services
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
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

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

Feature	IP Base	Enterprise Services
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
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

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

Feature	IP Base	Enterprise Services
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
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
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

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

Feature	IP Base	Enterprise Services
Network Time Protocol (NTP) master	Yes	Yes
NMSP Enhancements • GPS support for location • Location at switch level • Local timezone change • Name value pair • 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	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

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

Feature	IP Base	Enterprise Services
OSPF Support for Link State Advertisement (LSA) Throttling	Yes[3]	Yes
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
Policy Based Routing (PBR)	No	Yes
Policy-Based Routing (PBR) Recursive Next Hop	No	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

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

Feature	IP Base	Enterprise Services
PVLAN over EtherChannel	Yes	Yes
PVST + (Per VLAN Spanning Tree Plus)	Yes	Yes
Q-in-Q	Yes	Yes
QoS Packet Marking	Yes	Yes
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 Support[4]	Yes	Yes
Smart Port	Yes	Yes
SNMP (Simple Network Management Protocol)	Yes	Yes

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

Feature	IP Base	Enterprise Services
SNMP Inform Request	Yes	Yes
SNMP Manager	Yes	Yes
SNMPv2C	Yes	Yes
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

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

Feature	IP Base	Enterprise Services
Standby Supervisor Port Usage	Yes	Yes
Sticky Port Security	Yes	Yes
Sticky Port Security on Voice VLAN	Yes	Yes
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 SGT Exchange Protocol (SXP) IPv4	Yes	Yes
UDI - Unique Device Identifier	Yes	Yes
Uni-Directional Link Routing (UDLR)	Yes	Yes

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

Feature	IP Base	Enterprise Services
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 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
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
XML-PI	Yes	Yes

1. FHRP - Enhanced Object Tracking of IP SLAs is not supported in LANBase.
2. EEE 802.1t—An IEEE amendment to IEEE 802.1D that includes extended system ID, long path cost, and PortFast.
3. IP Base supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 200 dynamically learned routes.
4. Smart Install Director is not supported with VSS.

MIB Support

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

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

Features Not Supported on the Cisco Catalyst 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
- TrustSec: IEEE 802.1ae MACSec Layer 2 encryption
- TrustSec: IEEE 802.1ae MACSec encryption on user facing ports
- TrustSec: IEEE 802.1ae MACSec encryption on user facing ports SSO
- TrustSec: IEEE 802.1ae MACSec encryption between switch-to-switch links using Cisco SAP (Security Association Protocol)

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)
- Energywise
- 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

Note Smart Install Director is not supported with VSS.

Orderable Product Numbers

Table 6 Cisco IOS XE Software Release 3.4.0SG 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 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 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 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 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 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 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 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
Power Supply		

Table 6 Cisco IOS XE Software Release 3.4.0SG Product Numbers and Images for the Catalyst 4500-X Series Switches

Product Number	Description	Image
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		

Table 6 Cisco IOS XE Software Release 3.4.0SG Product Numbers and Images for the Catalyst 4500-X Series Switches

Product Number	Description	Image
S45XU-34-1512SG	CAT4500-X Universal image Cisco Catalyst 4500-X Cisco IOS Software XE Release 3.4.0 SG noncrypto universal image	cat4500e-universal.SPA.03.04.00.SG.151-2.SG.bin
S45XUK9-34-1512SG	CAT4500-X Universal crypto Cisco Catalyst 4500-X Cisco IOS Software XE Release 3.4.0 SG crypto universal image	cat4500e-universalk9.SPA.03.04.00.SG.151-2.SG.bin
C4500X-IPB	Catalyst 4500-X IP BASE software license (paper delivery)	N/A
C4500X-LIC=	Base product ID for software upgrade licenses on Catalyst 4500-X (paper delivery)	N/A
L-C4500X-LIC=	Catalyst 4500-X Base product ID for software upgrade licenses (electronic delivery)	N/A
C4500X-IP-ES (Paper delivery)	Catalyst 4500-X IP BASE to Enterprise Services upgrade license (paper delivery)	
L-C4500X-IP-ES (Electronic delivery)	Catalyst 4500-X IP BASE to Enterprise Services upgrade license (electronic delivery)	
C4500X-16P-IP-ES	Cisco IP Base to Enterprise Services Upgrade License (Paper Delivery) for Catalyst 4500-X (16-Port) Switch	N/A
L-C4500X-16P-IP-ES	Cisco IP Base to Enterprise Services Upgrade License (electronic delivery) for Catalyst 4500-X (16-Port) Switch	N/A

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 Software Features in Release IOS XE 3.4.2SG, page 30
- New Hardware Features in Release IOS XE 3.4.2SG, page 30
- New Software Features in Release IOS XE 3.4.0SG, page 30

- New Hardware Features in Release IOS XE 3.4.0SG, page 31

New Software Features in Release IOS XE 3.4.2SG

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

- Permanent Right-to-Use (PRTU) license

New Hardware Features in Release IOS XE 3.4.2SG

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

New Software Features in Release IOS XE 3.4.0SG

Release IOS XE 3.4.0SG provides the following new software features on the Catalyst 4500-X Series switch.

High Availability

- Virtual Switching System (VSS)

Security

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

Lower Total Cost of Ownership and Ease of Use

- Smart Install (Director Support)

Routing and Multicast Enhancements

- BGP Consistency Checker
- IPv6 BSR Scoped Zone support
- OSPFv3 Address Families
- OSPFv3 Time To Live Security

- Policy Based Routing: Recursive Next Hop

IPv6 Access Control

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

Other

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

New Hardware Features in Release IOS XE 3.4.0SG

Release IOS XE 3.4.0SG provides no new hardware on the Catalyst 4500-X Series switch.

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

Upgrading the System Software

If you are upgrading to IOS XE Version 3.4.0SG and are planning on using VSS, you must upgrade your ROMMON to IOS Version 15.0(1r)SG7. Else, leave the ROMMON at its default level.

You can upgrade a ROMMON image either through a console or telnet.

Limitations and Restrictions

These sections list the limitations and restrictions for the current release of Cisco IOS software on the Catalyst 4500-X Series switches.

- Starting with Release IOS XE 3.3.0SG and IOS 15.1(1)SG, 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

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

Caveats

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

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

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

Cisco Bug Search Tool

The Bug Search Tool (BST) is the online successor to Bug Toolkit and is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data

such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input. You can access the tool at: https://tools.cisco.com/bugsearch/ .

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

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

Resolved Caveats for Cisco IOS XE Release 3.4.8SG

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

Open Caveats for Cisco IOS XE Release 3.4.7SG

Bug ID	Headline
CSCuc49150	You cannot detach an input QoS policy from VSL member ports

Resolved Caveats for Cisco IOS XE Release 3.4.7SG

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

Open Caveats for Cisco IOS XE Release 3.4.6SG

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

Resolved Caveats for Cisco IOS XE Release 3.4.6SG

Bug ID	Headline
CSCtf75400	Wrong output for show platform software etherchannel port-channel n map
CSCuf52741	file verify auto always present in default-running-config

CSCul73513	Clock is not matching between server-client after leap configuration
CSCum56902	Sup7L-E FFM Crashes while removing the class-map
CSCun34745	\"ip ssh source-interface\" configuration missing after reload
CSCuo26294	Switch crashes with process FFM terminated abnormally
CSCuo28455	SMI - Custom group doesn't work for new PIDS not in the IBD database
CSCup84251	Crash on purge_app_tlv_and_notify
CSCuq01267	HSRP VMAC is not programmed after SSO in cat4k VSS setup
CSCuq04574	WS-C4500X-16 with 3.5.3E crashes due to SNMP polling
CSCuq80812	Incomplete ARP reply received on an active Flex Link port
CSCur21848	WCCP stops redirecting traffic when eighth port added to service group
CSCur23656	Cisco IOS and IOSd in IOS-XE : evaluation of SSLv3 POODLE vulnerability
CSCur58074	Some SFPs are not recognized when inserted into random ports on a switch
CSCur98467	VSL-MGMT access-list mac address changes after entire VSS reload
CSCus23266	C4500X deny ACE does not work correctly
CSCus47714	VSS active and standby MAC address teble can not synchronisation issue.
CSCus69731	IOS-XE for Nova device: glibc GHOST vulnerability - CVE-2015-0235

Open Caveats for Cisco IOS XE Release 3.4.5SG

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

Resolved Caveats for Cisco IOS XE Release 3.4.5SG

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

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

Open Caveats for Cisco IOS XE Release 3.4.4SG

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

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

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

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

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

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

  Workaround: None. CSCuc36612

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

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

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

  Workaround: None. CSCud39208

- 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

- 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

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

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

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

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

- 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.

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

  The exact triggers are unknown.

  Workaround: None. CSCuo37416

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

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

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

 ip igmp mroute-proxy Vlan2137
                      ^
% Invalid input detected at '^' marker.
```

  Workaround: Reapply the configuration when the switch reboots. CSCum71764

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

  Workaround: Do a switchover. CSCuo18934

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

  Workaround: None. CSCun83237

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

  Workaround: Disable netflow sampling. CSCtg00542

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

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

4500x_vss#show run | i mac add
 mac address-table static 03bf.ac10.0cb9 vlan 1 interface Te2/3  <--- Missing the 1/
```

  Upon reload, the config errors out

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

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

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

Resolved Caveats for Cisco IOS XE Release 3.4.4SG

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

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

  Workaround: None. CSCuj67614

- 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

- 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 debouce will be ineffective.

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

- A switch crashes on receiving a malformed LLDP packet.

  LLDP should be enabled.

  Workaround: None. CSCun66735

- Upon removing the active supervisor engine from a switch, multicast and unicast packet loss occur (for 60 seconds) until route convergence completes.

  Workaround: None. CSCun97605

Open Caveats for Cisco IOS XE Release 3.4.3SG

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

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

  Workaround: None. CSCth42248

- The **show ipv6 access-list** command displays incorrect match counts when multicast traffic is matched to an IPv6 access list that is attached to an SVI.

  Workaround: None. CSCth65129

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

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

- If you reboot a switch, the configured value of the interface MTU size for the elements of the port channel interface is invalid for IPv6 traffic.

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

  CSCto27085

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

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

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

  Workaround: None. CSCto46018

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

  Workaround: None. CSCtu37959

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

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

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

- When more than one Equal Cost Multipath (ECMP) is available on the downstream switch, and Mediatrace is invoked to provide flow statistics, the dynamic policy does not 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 a switchover is created on the Mediatrace responder, the dynamic access list created for a monitored flow tuple is not deleted. Although the Mediatrace initiator creates another set of dynamic access lists after the switchover, the old ones remain in the configuration.

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

  Workarounds:

  – If the switchover is scheduled, remove the scheduled session on the initiator, and reschedule the session after the new active supervisor engine boots on the responder.

  – After the new active supervisor engine boots, and provided the Mediatrace responder SSO is not planned, manually delete the stale dynamic access lists. CSCty75070

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

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

- 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

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

```
HARDWARE WATCHDOG
```

This message is not observed during a system bootup.

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

- 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 debouce 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. CSCuj67614

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

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

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

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

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

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

  CSCuc66206

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

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

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

  Workaround: None. CSCub33727
- The POST results on the VSS standby switch displayed by the **show diagnostic result module all detail** command indicate module number 1 rather than 11. The module number is not interpreted by Cisco IOS.

  Workaround: None. CSCuc73632
- The following (information-only) error message and traceback may occur during MFIB-to-platform state updates for Bidirectional PIM (*,G/m) entries associated with Bidirectional PIM rendezvous points:

```
%SYS-2-NOBLOCK: may_suspend with blocking disabled. -Process= "MFIB_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
- UDE does not function at 1Gbps.

  Workaround: None. CSCuj56314

Resolved Caveats for Cisco IOS XE Release 3.4.3SG

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

- All traffic is dropped on a port provided UDE is configured.

  Workaround: None. CSCui96407
- On systems performing multicast routing, a brief increase in CPU consumption occurs every few minutes. In large-scale environments, this CPU increase is more noticeable.

  Workaround: None. CSCub44553
- Following a switchover on VSS, CPU may remain high. The **show platform cpu packet statistics** command displays high usage due to “SA Miss.”

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

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

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

Workaround: None. CSCuj71597

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

  Wokarounds:

  – Ensure that the dot1x supplicant always authenticates before MAB.

  – Create MAB policies for dot1x hosts that do not supply a URL redirect. CSCui79988

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

  Workaround: None. CSCul00025

Open Caveats for Cisco IOS XE Release 3.4.2SG

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

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

  Workaround: None. CSCth42248

- The **show ipv6 access-list** command displays incorrect match counts when multicast traffic is matched to an IPv6 access list that is attached to an SVI.

  Workaround: None. CSCth65129

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

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

- If you reboot a switch, the configured value of the interface MTU size for the elements of the port channel interface is invalid for IPv6 traffic.

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

  CSCto27085

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

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

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

  Workaround: None. CSCto46018

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

  Workaround: None. CSCtu37959

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

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

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

- When more than one Equal Cost Multipath (ECMP) is available on the downstream switch, and Mediatrace is invoked to provide flow statistics, the dynamic policy does not 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 a switchover is created on the Mediatrace responder, the dynamic access list created for a monitored flow tuple is not deleted. Although the Mediatrace initiator creates another set of dynamic access lists after the switchover, the old ones remain in the configuration.

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

  Workarounds:

  – If the switchover is scheduled, remove the scheduled session on the initiator, and reschedule the session after the new active supervisor engine boots on the responder.

  – After the new active supervisor engine boots, and provided the Mediatrace responder SSO is not planned, manually delete the stale dynamic access lists. CSCty75070

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

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

- 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

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

  ```
  HARDWARE WATCHDOG
  ```

  This message is not observed during a system bootup.

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

- 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 debouce 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. CSCuj67614

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

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

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

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

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

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

  CSCuc66206

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

  Workaround: Turn off ICMP redirect 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

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

  – Incoming packets on the VSS standby port are directed to the CPU for host learning.

  – Layer 3 exceptions occur for packets arriving on the VSS standby port.

  – ACL logging occurs on the VSS standby port.

  Workaround: None. CSCub33727

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

  Workaround: None. CSCuc73632

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

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

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

  Workaround: None. CSCud39208

- All traffic is dropped on a port provided UDE is configured.

  Workaround: None. CSCui96407

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

  Workaround: Clear the MAC table. CSCuh50329

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

  Workaround: None.CSCug65204

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

  Workaround: CSCuh88726

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

  Workaround: None. CSCuj71597

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

  Wokarounds:

  – Ensure that the dot1x supplicant always authenticates before MAB.

  – Create MAB policies for dot1x hosts that do not supply a URL redirect. CSCui79988

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

  Workaround: None. CSCul00025

- UDE does not function at 1Gbps.

  Workaround: None. CSCuj56314

Resolved Caveats for Cisco IOS XE Release 3.4.2SG

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

- A GLC-GE-100FX pluggable may not operate when used in WS-X4624-SFP-E, WS-X4640-CSFP-E or WS-X4612-SFP-E modules.

  Workaround: None CSCui23911

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

  Workaround: Enter either the **no ip http server** or the **no ip http secure-server** command. This disables the http/s server. CSCui14525

- 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

Open Caveats for Cisco IOS XE Release 3.4.1SG

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

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

  Workaround: None. CSCth42248

- The **show ipv6 access-list** command displays incorrect match counts when multicast traffic is matched to an IPv6 access list that is attached to an SVI.

  Workaround: None. CSCth65129

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

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

- If you reboot a switch, the configured value of the interface MTU size for the elements of the port channel interface is invalid for IPv6 traffic.

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

  CSCto27085

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

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

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

Workaround: None. CSCto46018

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

  Workaround: None. CSCtu37959

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

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

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

- When more than one Equal Cost Multipath (ECMP) is available on the downstream switch, and Mediatrace is invoked to provide flow statistics, the dynamic policy does not 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 a switchover is created on the Mediatrace responder, the dynamic access list created for a monitored flow tuple is not deleted. Although the Mediatrace initiator creates another set of dynamic access lists after the switchover, the old ones remain in the configuration.

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

  Workarounds:

  – If the switchover is scheduled, remove the scheduled session on the initiator, and reschedule the session after the new active supervisor engine boots on the responder.

  – After the new active supervisor engine boots, and provided the Mediatrace responder SSO is not planned, manually delete the stale dynamic access lists. CSCty75070

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

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

- 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

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

  ```
  HARDWARE WATCHDOG
  ```

  This message is not observed during a system bootup.

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

- 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 debouce 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. CSCuj67614

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

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

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

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

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

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

  CSCuc66206

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

  Workaround: Turn off ICMP redirect 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

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

  Workaround: None. CSCub33727

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

  Workaround: None. CSCuc73632

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

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

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

  Workaround: None. CSCud39208

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

  Workaround: Enter either the **no ip http server** or the **no ip http secure-server** command. This disables the http/s server. CSCui14525

- A GLC-GE-100FX pluggable may not operate when used in WS-X4624-SFP-E, WS-X4640-CSFP-E or WS-X4612-SFP-E modules.

  Workaround: None CSCui23911

- All traffic is dropped on a port provided UDE is configured.

  Workaround: None. CSCui96407

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

  Workaround: Clear the MAC table. CSCuh50329

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

  Workaround: None.CSCug65204

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

  Workaround: CSCuh88726

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

  Workaround: None. CSCuj71597

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

  Wokarounds:

  – Ensure that the dot1x supplicant always authenticates before MAB.

  – Create MAB policies for dot1x hosts that do not supply a URL redirect. CSCui79988

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

  Workaround: None. CSCul00025

- UDE does not function at 1Gbps.

  Workaround: None. CSCuj56314

Resolved Caveats for Cisco IOS XE Release 3.4.1SG

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

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

  Workaround: Disable IGMP snooping. CSCuc65538

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

  Workaround: None. CSCua89658

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

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

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

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

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

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

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

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

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

  Workaround: Retain the trunk native VLAN as 1. CSCud05521

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

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

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

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

  CSCue62019

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

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

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

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

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

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

  CSCud55965

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

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

  S,G clears:
  - Minimize Layer 2 or Layer 3 topology changes that would require multicast reconvergence.
  - Avoid manually clearing mroutes. CSCua62262

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

  Workaround: Once the problem occurs, reboot the switch.

  Disabling Fa1 prevents the problem. CSCue76243

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

  Workaround: None. CSCue96534

- When the Fa1 on a switch running IOS Release XE 3.3.0SG or 3.4.0SG receives a unicast frame whose destination MAC address is not Fa1, traffic is redirected back out of Fa1 instead of being dropped.

  Workaround: None. CSCuc12774

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

  Workaround: Use SNMPWALK. CSCtz67068

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

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

  Workaround: Avoid scripted CLI. CSCtz19897

- MAC address learning does not occur on dot1q-tunnel ports.

  Workaround: None. CSCub01918

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

  Workaround: Shorten the dACL name. CSCug78653

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

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

Open Caveats for Cisco IOS XE Release 3.4.0SG

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

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

  Workaround: None. CSCth42248

- The **show ipv6 access-list** command displays incorrect match counts when multicast traffic is matched to an IPv6 access list that is attached to an SVI.

  Workaround: None. CSCth65129

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

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

- If you reboot a switch, the configured value of the interface MTU size for the elements of the port channel interface is invalid for IPv6 traffic.

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

  CSCto27085

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

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

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

  Workaround: None. CSCto46018

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

  Workaround: None. CSCtu37959

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

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

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

- When more than one Equal Cost Multipath (ECMP) is available on the downstream switch, and Mediatrace is invoked to provide flow statistics, the dynamic policy does not 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 a switchover is created on the Mediatrace responder, the dynamic access list created for a monitored flow tuple is not deleted. Although the Mediatrace initiator creates another set of dynamic access lists after the switchover, the old ones remain in the configuration.

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

  Workarounds:

  – If the switchover is scheduled, remove the scheduled session on the initiator, and reschedule the session after the new active supervisor engine boots on the responder.

  – After the new active supervisor engine boots, and provided the Mediatrace responder SSO is not planned, manually delete the stale dynamic access lists. CSCty75070

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

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

- 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

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

  ```
  HARDWARE WATCHDOG
  ```

  This message is not observed during a system bootup.

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

- 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 is 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. CSCuj67614

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

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

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

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

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

  Workaround: None. Reduce the number of VLANs created at one time.

  CSCuc66206

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

  Workaround: Turn off ICMP redirect 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

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

– ACL logging occurs on the VSS standby port.

Workaround: None. CSCub33727

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

  Workaround: None. CSCuc73632

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

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

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

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

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

  Workaround: None. CSCud39208

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

  Workaround: None. CSCua89658

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

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

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

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

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

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

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

  Workaround: Retain the trunk native VLAN as 1. CSCud05521

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

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

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

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

  CSCue62019

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

  – a fast stream of traffic matches the URL redirect ACL as IPDT clears an address,

  – a traffic stream matches the URL redirect ACL and no URL redirect policy is installed for that IP address,

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

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

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

  Workaround: Shorten the dACL name. CSCug78653

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

  Workaround: Disable IGMP snooping. CSCuc65538

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

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

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

  CSCud55965

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

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

  – Extend the receiver-less S,G duration (e.g. ip pim sparse sg-expiry-timer <big value>).

  – If sources are varied, try to minimize them.

  – If some static sources send infrequently, extend the expiry timer to cover the gaps in the packet stream.

  – If some receivers are unreliable, consider static joins.

  S,G clears:

  – Minimize Layer 2 or Layer 3 topology changes that would require multicast reconvergence.

  - Avoid manually clearing mroutes. CSCua62262

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

  Workaround: Once the problem occurs, reboot the switch.

  Disabling Fa1 prevents the problem. CSCue76243

- A switch running IOS Release 15.1(1)SG, 15.1(1)SG1, 15.1(1)SG2, or 15.1(2)SG, drops some fragmented packets that are routed through the switch. Bridged traffic is unaffected.

  Workaround: None. CSCue96534

- When the Fa1 on a switch running IOS Release XE 3.3.0SG or 3.4.0SG receives a unicast frame whose destination MAC address is not Fa1, traffic is redirected back out of Fa1 instead of being dropped.

  Workaround: None. CSCuc12774

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

  Workaround: Use SNMPWALK. CSCtz67068

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

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

  Workaround: Avoid scripted CLI. CSCtz19897

- MAC address learning does not occur on dot1q-tunnel ports.

  Workaround: None. CSCub01918

- A GLC-GE-100FX pluggable may not operate when used in WS-X4624-SFP-E, WS-X4640-CSFP-E or WS-X4612-SFP-E modules.

  Workaround: None CSCui23911

- All traffic is dropped on a port provided UDE is configured.

  Workaround: None. CSCui96407

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

  Workaround: Clear the MAC table. CSCuh50329

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

  Workaround: None.CSCug65204

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

  Workaround: CSCuh88726

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

  Workaround: None. CSCul00025

Resolved Caveats for Cisco IOS XE Release 3.4.0SG

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

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

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

  Workaround: Enter **shut**, then **no shut** on the port. CSCts29515

- A WS-C4500-X Series switch will fail when you use the **switchport** command to convert ports from Layer 3 to Layer 2, if the former is configured with IPv4 and IPv6 ACLs (each with 500 ACEs).

  Workaround: Enter the **default interface te** command in global configuration mode before you enter the **switchport** command. CSCty52629

- A Catalyst 4500-X switch fails if you enter **show memory debug leak** on the console executing **show memory detailed process iosd debug leaks** from another Telnet session.

  Workaround: Avoid running both commands simultaneously. CSCty27680

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.

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

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

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

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

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

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.

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