Release Notes for the Catalyst 4500E Series Switch, Cisco IOS XE 3.3.xXO

Current release: IOS XE 3.3.2XO—August 20, 2014

Prior release: IOS XE 3.3.1XO, IOS XE 3.3.0XO—August 14, 2013

This release note describes the features, modifications, and caveats for the Cisco IOS XE 3.3.*x*XO software on the Catalyst 4500E series switch with Supervisor Engine 8-E.

The new Cisco® Catalyst® 4500E Supervisor Engine 8-E extends one policy, one management, one network to the world's most widely deployed modular access switch. This brings convergence of wired and wireless (not available in the first release of convergence, IOS XE 3.3.0XO in networks on a single platform while providing unprecedented investment protection. It ushers in a new converged architecture that is simple, resilient, and secure.

The Cisco Catalyst 4500E Switch with Supervisor Engine 8-E is an extremely scalable and feature-rich modular access platform built to meet current and future network demand, and including gigabit desktop:

Converged Access

- Hardware-readiness for built-in wireless controller with single software image for wired and wireless infrastructure
- Hardware-readiness for delivery of up to 928 Gbps system bandwidth and nonblocking 48 Gbps per slot
- Support for up to 20 G wireless throughput, 50 access points, and 2000 wireless clients on a single system and 250 access points and 4000 clients for multiswitch controllerless deployment
- Eight nonblocking 10 Gigabit Ethernet (Small Form-Factor Pluggable Plus [SFP+]) future-proofed uplinks with field-programmable gate array (FPGA) devices to support next-generation protocols
- Ability of 4500E chassis with Supervisor Engine 8-E to scale up to 384 Gigabit copper ports, 200 Gigabit fiber ports, or 104 10 Gigabit ports in non-VSS mode

Infrastructure Services

- Maximum resiliency with redundant components, Nonstop Forwarding/Stateful Switchover (NSF/SSO)
- Network virtualization through Multi-Virtual Route Forwarding (VRF) and Easy Virtual Networking (EVN) technology for Layer 3 segmentation

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

- Power over Ethernet Plus (PoE+; 30 W) and Cisco Universal PoE (UPOE; 60 W) capabilities on all line-card slots

Investment Protection and Reduced Total Cost of Ownership

- Full backward compatibility with 6-, 24-, and 48-Gbps line cards with no performance degradation
- Compatibility with all shipping Cisco Catalyst 4500 chassis, line cards, and power supplies, thus providing full investment protection

Cisco Services

- Optimized application performance through deep visibility with flexible NetFlow (FNF), supporting rich Layer 2, 3, and 4 information (MAC, VLAN, and TCP flags) and synthetic traffic with IP service-level agreements
- Medianet capabilities for video quality of service (QoS), monitoring, and security

Support for Cisco IOS XE Release 3.3.0XO follows the standard Cisco Systems® support policy, available at

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

For more information on the Catalyst 4500E series switches, visit the following URL:

http://www.cisco.com/go/cat4500/docs

Contents

This publication consists of these sections:

Cisco IOS Software Packaging

The Enterprise Services image supports all Cisco Catalyst 4500 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), GLBP, and policy-based routing (PBR).

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

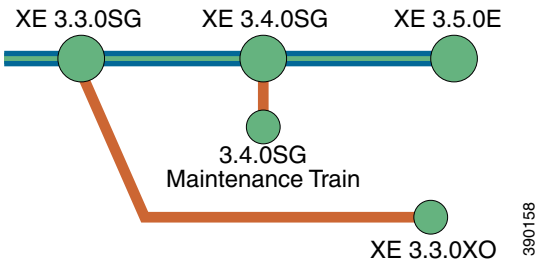
Cisco IOS XE Release Strategy

Sup8-E is introduced with Cisco IOS Release XE 3.3.0XO, which has feature parity with Release XE 3.3.0SG. Sup8-E support will be integrated into XE 3.6.0E, which will be an extended maintenance release.

Note Sup8-E is not supported on Release XE 3.3.nSG, XE 3.4.nSG, or XE 3.5.0E.

Figure 1 displays the one active train, 3.4.0SG.

Figure 1 Software Release Strategy for Catalyst 4500 Series Switch, Release XE 3.3.0XO



Topics include:

- Feature Support by Image Type, page 3
- Appendix 1, “Features Not Supported on the Cisco Catalyst 4500E Series Switch, IOS Release XE 3.3.0XO”
- Orderable Product Numbers, page 24

Feature Support by Image Type

Table 1 is a detailed list of features supported on Catalyst 4500E Supervisor Engine 8-E running Cisco IOS XE Release 3.3.0XO categorized by image type.

Note Feature parity exists between this release and Release 3.3.0SG.

Please visit Feature Navigator for package details:

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

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
2-way Community Private VLANs	No	Yes	Yes
8-Way CEF Load Balancing	Yes	Yes	Yes
10 Gigabit Uplink Use	Yes	Yes	Yes
AAA Server Group	Yes	Yes	Yes
AAA Server Group Based on DNIS	Yes	Yes	Yes
ACL - Improved Merging Algorithm	Yes	Yes	Yes
ACL Logging	Yes	Yes	Yes
ACL Policy Enhancements	Yes	Yes	Yes
ACL Sequence Numbering	Yes	Yes	Yes
Address Resolution Protocol (ARP)	Yes	Yes	Yes
ANCP Client	No	Yes	Yes
ANSI TIA-1057 LLDP - MED Location Extension	Yes	Yes	Yes
ANSI TIA-1057 LLDP - MED Support	Yes	Yes	Yes
ARP Optimization	Yes	Yes	Yes
Auto QoS	Yes	Yes	Yes
Auto SmartPorts	Yes	Yes	Yes
Auto-MDIX	Yes	Yes	Yes
Auto-Voice VLAN (part of Auto QoS)	Yes	Yes	Yes
AutoInstall Using DHCP for LAN Interfaces	Yes	Yes	Yes
AutoQoS - VoIP	Yes	Yes	Yes
AutoRP Enhancement	No	Yes	Yes
BGP	No	No	Yes
BGP 4	No	No	Yes
BGP 4 4Byte ASN (CnH)	No	No	Yes
BGP 4 Multipath Support	No	No	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
BGP 4 Prefix Filter and In-bound Route Maps	No	No	Yes
BGP 4 Soft Config	No	No	Yes
BGP Conditional Route Injection	No	No	Yes
BGP Configuration Using Peer Templates	No	No	Yes
BGP Dynamic Update Peer-Groups	No	No	Yes
BGP Increased Support of Numbered as-path Access Lists to 500	No	No	Yes
BGP Link Bandwidth	No	No	Yes
BGP Neighbor Policy	No	No	Yes
BGP Prefix-Based Outbound Route Filtering	No	No	Yes
BGP Restart Neighbor Session After max-prefix Limit Reached	No	No	Yes
BGP Route-Map Continue	No	No	Yes
BGP Route-Map Continue Support for Outbound Policy	No	No	Yes
BGP Soft Rest	No	No	Yes
BGP Wildcard	No	No	Yes
Bidirectional PIM (IPv4 only)	No	Yes	Yes
Boot Config	Yes	Yes	Yes
Broadcast/Multicast Suppression	Yes	Yes	Yes
Call Home	No	Yes	Yes
CDP (Cisco Discovery Protocol) Version 2	Yes	Yes	Yes
CDP Enhancement - Host presence TLV	Yes	Yes	Yes
CEF/dCEF - Cisco Express Forwarding	Yes	Yes	Yes
CEFv6 Switching for 6to4 Tunnels	No	Yes	Yes
CEFv6/dCEFv6 - Cisco Express Forwarding	Yes	Yes	Yes
CFM/IEEE 802.1ag - D8.1 standard Compliant CFM, Y.1731 multicast LBM / AIS / RDI / LCK, IP SLA for Ethernet	Yes	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
CGMP - Cisco Group Management Protocol	No	Yes	Yes
Cisco IOS Scripting w/Tcl	Yes	Yes	Yes
CiscoView Autonomous Device Manager (ADP)	No	Yes	Yes
Class Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)	Yes	Yes	Yes
Class-Based Marking	Yes	Yes	Yes
Class-Based Policing	Yes	Yes	Yes
Class-Based Shaping	Yes	Yes	Yes
Clear Counters Per Port	Yes	Yes	Yes
CLI String Search	Yes	Yes	Yes
CNS	Yes	Yes	Yes
CNS - Configuration Agent	Yes	Yes	Yes
CNS - Event Agent	Yes	Yes	Yes
CNS - Image Agent	Yes	Yes	Yes
CNS - Interactive CLI	Yes	Yes	Yes
CNS Config Retrieve Enhancement with Retry and Interval	Yes	Yes	Yes
Command Scheduler (Kron)	Yes	Yes	Yes
Command Scheduler (Kron) Policy for System Startup	Yes	Yes	Yes
Commented IP Access List Entries	Yes	Yes	Yes
Community Private VLAN	No	Yes	Yes
Configuration Change Tracking Identifier	Yes	Yes	Yes
Configuration Change Notification and Logging	No	Yes	Yes
Configuration Replace and Configuration Rollback	Yes	Yes	Yes
Configuration Rollback Confirmed Change	Yes	Yes	Yes
Contextual Configuration Diff Utility	Yes	Yes	Yes
Control Plane Policing (Copp)	Yes	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
CPU Optimization for Layer 3 Multicast Control Packets	Yes	Yes	Yes
Critical Authorization for Voice and Data	Yes	Yes	Yes
DAI (Dynamic ARP inspection)	Yes	Yes	Yes
DBL (Dynamic Buffer Limiting) - Selective DBL	Yes	Yes	Yes
Debounce Timer per Port	Yes	Yes	Yes
Default Passive Interface	No	Yes	Yes
DHCP Client	Yes	Yes	Yes
DHCP Configurable DHCP Client	Yes	Yes	Yes
DHCPv6 Relay Agent notification for Prefix Delegation	Yes	Yes	Yes
DHCP Option 82, Pass Through	Yes	Yes	Yes
DHCP Server	Yes	Yes	Yes
DHCP Snooping	Yes	Yes	Yes
DHCPv6 Ethernet Remote ID option	Yes	Yes	Yes
DHCPv6 Relay - Reload persistent Interface ID option	Yes	Yes	Yes
DHCPv6 Repackaging	Yes	Yes	Yes
DSCP/CoS via LLDP	Yes	Yes	Yes
Duplication Location Reporting Issue	No	Yes	Yes
Dynamic Trunking Protocol (DTP)	Yes	Yes	Yes
Easy Virtual Network (EVN)	No	No	Yes
EIGRP	No	No	Yes
EIGRP Service Advertisement Framework	Yes	Yes	Yes
EIGRP Stub Routing	No	Yes	Yes
Embedded Event Manager (EEM) 3.2	No	Yes	Yes
Embedded Syslog Manager (ESM)	Yes	Yes	Yes
EnergyWise 2.5	Yes	Yes	Yes
Enhanced PoE Support (Additional Wattage Range)	Yes	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
Entity API for Physical and Logical Mgd Entities	Yes	Yes	Yes
ErrDisable timeout	Yes	Yes	Yes
EtherChannel	Yes	Yes	Yes
EtherChannel Flexible PAgP	Yes	Yes	Yes
EtherChannel Single Port Channel	Yes	Yes	Yes
Fast EtherChannel (FEC)	Yes	Yes	Yes
FHRP - Enhanced Object Tracking of IP SLAs	Yes	Yes	Yes
FHRP - Enhanced Object Tracking integration with EEM	Yes	Yes	Yes
FHRP - GLBP - IP Redundancy API	No	Yes	Yes
FHRP - HSRP - Hot Standby Router Protocol V2	No	Yes	Yes
FHRP - Object Tracking List	No	Yes	Yes
Filter-ID Based ACL Application	Yes	Yes	Yes
FIPS 140-2/3 Level 2 Certification	Yes	Yes	Yes
Flexible Netflow - Ethertype	No	No	Yes
Flexible NetFlow - Full Flow support	No	Yes	Yes
Flexible NetFlow - Ingress support	No	Yes	Yes
Flexible NetFlow - IPv4 Unicast Flows	No	Yes	Yes
Flexible NetFlow - IPv6 Unicast Flows	No	Yes	Yes
Flexible NetFlow - Layer 2 Fields	No	Yes	Yes
Flexible NetFlow - Multiple User Defined Caches	No	Yes	Yes
Flexible NetFlow - NetFlow Export over IPv4	No	Yes	Yes
Flexible NetFlow - NetFlow v5 Export Protocol	No	Yes	Yes
Flexible NetFlow - NetFlow v9 Export Format	No	Yes	Yes
Flexible Netflow - Username	No	No	Yes
Flexible NetFlow - VLAN ID support	No	Yes	Yes
Flex Links+(VLAN Load balancing)	Yes	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
Forced 10/100 Autonegotiation	Yes	Yes	Yes
FTP Support for Downloading Software Images	Yes	Yes	Yes
Gateway Load Balancing Protocol GLBP	No	Yes	Yes
Generic Routing Encapsulation (GRE)	No	Yes	Yes
GOLD Online Diagnostics	Yes	Yes	Yes
HSRP - Hot Standby Router Protocol	No	Yes	Yes
HSRPv2 for IPv6 Global Address Support	No	Yes	Yes
HTTP Security	Yes	Yes	Yes
HTTP TACAC+ Accounting support	Yes	Yes	Yes
IEEE 802.1ab LLDP (Link Layer Discovery Protocol)	Yes	Yes	Yes
IEEE 802.1ab LLDP/LLDP-MED	Yes	Yes	Yes
IEEE 802.1ab LLDP enhancements (PoE+Layer 2 COS)	Yes	No	No
IEEE 802.1p Support	Yes	Yes	Yes
IEEE 802.1Q VLAN Trunking	Yes	Yes	Yes
IEEE 802.1s Multiple Spanning Tree (MST) Standard Compliance	Yes	Yes	Yes
IEEE 802.1s VLAN Multiple Spanning Trees	Yes	Yes	Yes
IEEE 802.1t[1]	Yes	Yes	Yes
IEEE 802.1w Spanning Tree Rapid Reconfiguration	Yes	Yes	Yes
IEEE 802.1x Auth Fail Open (Critical Ports)	Yes	Yes	Yes
IEEE 802.1x Auth Fail VLAN	Yes	Yes	Yes
IEEE 802.1x Flexible Authentication	Yes	Yes	Yes
IEEE 802.1x Multiple Authentication	Yes	Yes	Yes
IEEE 802.1x Open Authentication	Yes	Yes	Yes
IEEE 802.1X with User Distribution	Yes	Yes	Yes
IEEE 802.1x VLAN Assignment	Yes	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
IEEE 802.1x VLAN User Group Distribution	Yes	Yes	Yes
IEEE 802.1x Wake on LAN Support	Yes	Yes	Yes
IEEE 802.1x Authenticator	Yes	Yes	Yes
IEEE 802.1x Fallback support	Yes	Yes	Yes
IEEE 802.1x Guest VLAN	Yes	Yes	Yes
IEEE 802.1x Multi-Domain Authentication	Yes	Yes	Yes
IEEE 802.1x Private Guest VLAN	Yes	Yes	Yes
IEEE 802.1x Private VLAN Assignment	Yes	Yes	Yes
IEEE 802.1x RADIUS Accounting	Yes	Yes	Yes
IEEE 802.1x RADIUS-Supplied Session Timeout	Yes	Yes	Yes
IEEE 802.1x with ACL Assignments	Yes	Yes	Yes
IEEE 802.1x with Port Security	Yes	Yes	Yes
IEEE 802.3ad Link Aggregation (LACP)	Yes	Yes	Yes
IEEE 802.3ad Link Aggregation (LACP) Port-Channel Standalone Disable	Yes	Yes	Yes
IEEE 802.3af PoE (Power over Ethernet)	Yes	Yes	Yes
IEEE 802.3x Flow Control	Yes	Yes	Yes
IGMP Fast Leave	Yes	Yes	Yes
IGMP Filtering	Yes	Yes	Yes
IGMP Snooping	Yes	Yes	Yes
IGMP Version 1	Yes	Yes	Yes
IGMP Version 2	Yes	Yes	Yes
IGMP Version 3	Yes	Yes	Yes
IGMP Version 3 - Explicit Tracking of Hosts, Groups, and Channels	Yes	Yes	Yes
IGMPv3 Host Stack	Yes	Yes	Yes
IGMPv3 Snooping: Full Support	Yes	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
Image Verification	Yes	Yes	Yes
Individual SNMP Trap Support	Yes	Yes	Yes
Inline Power Auto Negotiation	Yes	Yes	Yes
Inline Power Management	Yes	Yes	Yes
Interface Index Persistence	Yes	Yes	Yes
Interface Range Specification	Yes	Yes	Yes
IOS Based Device Profiling	No	Yes	Yes
IP Enhanced IGRP Route Authentication	No	No	Yes
IP Event Dampening	No	Yes	Yes
IP Multicast Load Splitting - Equal Cost Multipath (ECMP) using S, G and Next-hop	No	No	Yes
IP Multicast Load Splitting across Equal-Cost Paths	No	Yes	Yes
IP Named Access Control List	Yes	Yes	Yes
IPv6 Tunnels (in software)	No	Yes	Yes
IP Routing	Yes	Yes	Yes
IP SLAs - DHCP Operations	No	Yes	Yes
IP SLAs - Distribution of Statistics	No	Yes	Yes
IP SLAs - DNS Operation	No	Yes	Yes
IP SLAs - FTP Operation	No	Yes	Yes
IP SLA - HTTP Operation	No	Yes	Yes
IP SLAs - ICMP Echo Operation	No	Yes	Yes
IP SLAs - ICMP Path Echo Operation	No	Yes	Yes
IP SLAs - Multi Operation Scheduler	No	Yes	Yes
IP SLAs - One Way Measurement	No	Yes	Yes
IP SLAs - Path Jitter Operation	No	Yes	Yes
IP SLAs - Random Scheduler	No	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
IP SLAs - Reaction Threshold	No	Yes	Yes
IP SLAs - Responder	No	Yes	Yes
IP SLAs - Scheduler	No	Yes	Yes
IP SLAs - Sub-millisecond Accuracy Improvements	No	Yes	Yes
IP SLAs - TCP Connect Operation	No	Yes	Yes
IP SLAs - UDP Based VoIP Operation	No	Yes	Yes
IP SLAs - UDP Echo Operation	No	Yes	Yes
IP SLAs - UDP Jitter Operation	No	Yes	Yes
IP SLAs - VoIP Threshold Traps	No	Yes	Yes
IP Summary Address for RIPv2	No	Yes	Yes
IP Unnumbered for VLAN-SVI interfaces	No	Yes	Yes
IPSG (IP Source Guard) v4	Yes	Yes	Yes
IPSG (IP Source Guard) v4 for Static Hosts	Yes	Yes	Yes
IPv4 Routing: Static Hosts/Default Gateway	Yes	Yes	Yes
IPv6 BGP	No	No	Yes
IPv6 CNS Agents	Yes	Yes	Yes
IPv6 Config Logger	Yes	Yes	Yes
IPv6 HSRP	No	Yes	Yes
IPv6 HTTP(S)	Yes	Yes	Yes
IPv6 Interface Statistics	Yes	Yes	Yes
IPv6 IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	No	Yes	Yes
IPv6 TCL	Yes	Yes	Yes
IPv6 (Internet Protocol Version 6)	Yes	Yes	Yes
IPv6 Interface Statistics	Yes	Yes	Yes
IPv6 Access Services: DHCPv6 Relay Agent	No	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
IPv6 MLD Snooping v1 and v2	Yes	Yes	Yes
IPv6 MTU Path Discovery	Yes	Yes	Yes
IPv6 Multicast	No	Yes	Yes
IPv6 Multicast: Bootstrap Router (BSR)	No	Yes	Yes
IPv6 Multicast: Explicit Tracking of Receivers	No	Yes	Yes
IPv6 Multicast: MLD Access Group	No	Yes	Yes
IPv6 Multicast: Multicast Listener Discovery (MLD) Protocol, Versions 1 and 2	No	Yes	Yes
IPv6 Multicast: PIM Accept Register	No	Yes	Yes
IPv6 Multicast: PIM Embedded RP Support	No	Yes	Yes
IPv6 Multicast: PIM Source-Specific Multicast (PIM-SSM)	No	Yes	Yes
IPv6 Multicast: PIM Sparse Mode (PIM-SM)	No	Yes	Yes
IPv6 Multicast: Routable Address Hello Option	No	Yes	Yes
IPv6 Multicast: RPF Flooding of Bootstrap Router (BSR) Packets	No	Yes	Yes
IPv6 Multicast: Scope Boundaries	No	Yes	Yes
IPv6 Neighbor Discovery	Yes	Yes	Yes
IPv6 PACL	Yes	Yes	Yes
IPv6 RA Guard	Yes	Yes	Yes
IPV6 Router Advertisement (RA) Guard	Yes	Yes	Yes
IPv6 Routing - EIGRP Support	No	No	Yes
IPv6 Routing: OSPF for IPv6 (OSPFv3)	No	Yes[2]	Yes
IPv6 Routing: RIP for IPv6 (RIPng)	No	Yes	Yes
IPv6 Routing: Route Redistribution	No	Yes	Yes
IPv6 Routing: Static Routing	Yes	Yes	Yes
IPv6 Security: Secure Shell SSH support over IPv6	Yes	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
IPv6 Services: AAAA DNS Lookups over an IPv4 Transport	No	Yes	Yes
IPv6 Services: Cisco Discovery Protocol (CDP) - IPv6 Address Family Support for Neighbor Information	Yes	Yes	Yes
IPv6 Services: DNS Lookups over an IPv6 Transport	Yes	Yes	Yes
IPv6 Services: Extended Access Control Lists	Yes	Yes	Yes
IPv6 Services: Standard Access Control Lists	Yes	Yes	Yes
IPv6 Stateless Auto-configuration	Yes	Yes	Yes
IPv6 Switching: CEF Support	No	Yes	Yes
IPv6 Switching: CEFv6 Switched Automatic IPv4-compatible Tunnels (in software)	No	Yes	Yes
IPv6 Switching: CEFv6 Switched ISATAP Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: Automatic 6to4 Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: Automatic IPv4-compatible Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: ISATAP Tunnel Support (in software)	No	Yes	Yes
IPv6 Tunneling: Manually Configured IPv6 over IPv4 Tunnels (in software)	No	Yes	Yes
IPv6: Anycast Address	Yes	Yes	Yes
IPv6: ICMPv6	Yes	Yes	Yes
IPv6: ICMPv6 Redirect	Yes	Yes	Yes
IPv6: Neighbor Discovery Duplicate Address Detection	Yes	Yes	Yes
IPsecv3/IKEv2 (for management traffic only)	Yes	Yes	Yes
IPv6 OSPFv3 NSF/SSO	No	Yes[2]	Yes
IPv6 OSPFv3 Fast Convergence	No	Yes[2]	Yes
IS-IS for IPv4 and IPv6	No	No	Yes
IS-IS Caching of Redistributed Routes	No	No	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
IS-IS MIB	No	No	Yes
IS-IS Multiarea Support	No	No	Yes
Jumbo Frames	Yes	Yes	Yes
Layer 2 Control Packet	Yes	Yes	Yes
Layer 2 Protocol Tunneling (L2PT)	Yes	Yes	Yes
Layer 2 Traceroute	No	Yes	Yes
Layer 3 Multicast Routing (PIM SM, SSM, Bidir)	No	Yes	Yes
Link State Tracking	Yes	Yes	Yes
Loadsharing IP packets over more than six parallel paths	Yes	Yes	Yes
Local Proxy ARP	Yes	Yes	Yes
Location MIBs	Yes	Yes	Yes
MAB with Configurable User Name/Password	Yes	Yes	Yes
MAB for Voice VLAN	Yes	Yes	Yes
MAC Address Notification	Yes	Yes	Yes
MAC Authentication Bypass	Yes	Yes	Yes
MAC Move and Replace	Yes	Yes	Yes
Management IPV6 port	Yes	Yes	Yes
Medianet: AutoQoS SRND4 Macro	No	Yes	Yes
Medianet: Integrated Video Traffic Simulator (hardware-assisted IP SLA); IPSLA generator and responder	No	Yes	Yes
Medianet: Flow Metadata	No	Yes	Yes
Medianet: Media Service Proxy	No	Yes	Yes
Medianet: Media Monitoring (Performance Monitoring and Mediatrace)	No	Yes	Yes
Memory Threshold Notifications	Yes	Yes	Yes
Microflow policers	No	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
Modular QoS CLI (MQC)	Yes	Yes	Yes
Multi-authentication and VLAN Assignment	Yes	Yes	Yes
Multi-VRF Support (VRF lite)	No	No	Yes
Multicast BGP (MBGP)	No	No	Yes
Multicast Fast Switching Performance Improvement	No	Yes	Yes
Multicast Routing Monitor (MRM)	No	No	Yes
Multicast Source Discovery Protocol (MSDP)	No	Yes	Yes
Multicast Subsecond Convergence	No	Yes	Yes
NAC - L2 IEEE 802.1x	Yes	Yes	Yes
NAC - L2 IP	Yes	Yes	Yes
ND Cache Limit/Interface	No	Yes	Yes
NEAT Enhancement: Re-Enabling BPDU Guard Based on User Configuration	Yes	Yes	Yes
NETCONF over SSHv2	Yes	Yes	Yes
Network Edge Access Topology (NEAT)	Yes	Yes	Yes
Network Time Protocol (NTP)	Yes	Yes	Yes
Network Time Protocol (NTP) master	Yes	Yes	Yes
NMSP Enhancements • GPS support for location • Location at switch level • Local timezone change • Name value pair • Priority settings for MIBs	No	Yes	Yes
No Service Password Recovery	Yes	Yes	Yes
No. of VLAN Support	2048	4096	4096
NSF - BGP	No	No	Yes
NSF - EIGRP	No	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
NSF - OSPF (version 2 only)	No	Yes	Yes
NSF/SSO (Nonstop Forwarding with Stateful Switchover)	No	Yes	Yes
NTP for IPv6	Yes	Yes	Yes
NTP for VRF aware	No	No	Yes
Onboard Failure Logging (OBFL)	Yes	Yes	Yes
OSPF	No	Yes[2]	Yes
OSPF v3 Authentication	No	Yes[2]	Yes
OSPF Flooding Reduction	No	Yes[2]	Yes
OSPF for Routed Access	No	Yes	Yes
OSPF Incremental Shortest Path First (i-SPF) Support	No	Yes[2]	Yes
OSPF Link State Database Overload Protection	No	Yes[2]	Yes
OSPF Not-So-Stubby Areas (NSSA)	No	Yes[2]	Yes
OSPF Packet Pacing	No	Yes[2]	Yes
OSPF Shortest Paths First Throttling	No	Yes[2]	Yes
OSPF Stub Router Advertisement	No	Yes[2]	Yes
OSPF Support for Fast Hellos	No	Yes[2]	Yes
OSPF Support for Link State Advertisement (LSA) Throttling	No	Yes[2]	Yes
OSPF Support for Multi-VRF on CE Routers	No	Yes[2]	Yes
OSPF Update Packet-Pacing Configurable Timers	No	Yes[2]	Yes
Out-of-band Management Port	Yes	Yes	Yes
Per Intf IGMP State Limit	Yes	Yes	Yes
Per Intf MrouteState Limit	Yes	Yes	Yes
Per Port Per VLAN Policing	Yes	Yes	Yes
Per-User ACL Support for 802.1X/MAB/Webauth users	Yes	Yes	Yes
Per-VLAN Learning	Yes	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
PIM Dense Mode State Refresh	No	Yes	Yes
PIM Multicast Scalability	No	Yes	Yes
PIM Version 1	No	Yes	Yes
PIM Version 2	No	Yes	Yes
PoEP via LLDP	Yes	Yes	Yes
Policy Based Routing (PBR)	No	No	Yes
Port Security	Yes	Yes	Yes
Port Security on Etherchannel Trunk Port	Yes	Yes	Yes
Pragmatic General Multicast (PGM)	No	Yes	Yes
Priority Queueing (PQ)	Yes	Yes	Yes
Private VLAN Promiscuous Trunk Port	Yes	Yes	Yes
Private VLAN Trunk Ports	Yes	Yes	Yes
Private VLANs	Yes	Yes	Yes
Propagation of Location Info over CDP	Yes	Yes	Yes
PVLAN over EtherChannel	Yes	Yes	Yes
PVST + (Per VLAN Spanning Tree Plus)	Yes	Yes	Yes
Q-in-Q	No	Yes	Yes
QoS Packet Marking	Yes	Yes	Yes
QoS Priority Percentage CLI Support	Yes	Yes	Yes
RADIUS	Yes	Yes	Yes
RADIUS Attribute 44 (Accounting Session ID) in Access Requests	Yes	Yes	Yes
RADIUS Change of Authorization	Yes	Yes	Yes
Rapid PVST+ Dispute Mechanism	Yes	Yes	Yes
Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)	Yes	Yes	Yes
Reduced MAC Address Usage	Yes	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
Redundancy Facility Protocol	Yes	Yes	Yes
Remote SPAN (RSPAN)	Yes	Yes	Yes
REP (Resilient Ethernet Protocol)	Yes	Yes	Yes
REP - No Edge Neighbor Enhancement	Yes	Yes	Yes
RIP v1	No	Yes	Yes
RMON events and alarms	Yes	Yes	Yes
Secure Copy (SCP)	Yes	Yes	Yes
Secure Shell SSH Version 1 Integrated Client	Yes	Yes	Yes
Secure Shell SSH Version 1 Server Support	Yes	Yes	Yes
Secure Shell SSH Version 2 Client Support	Yes	Yes	Yes
Secure Shell SSH Version 2 Server Support	Yes	Yes	Yes
Single Rate 3-Color Marker for Traffic Policing	Yes	Yes	Yes
Smart Port	Yes	Yes	Yes
SNMP (Simple Network Management Protocol)	Yes	Yes	Yes
SNMP Inform Request	Yes	Yes	Yes
SNMP Manager	Yes	Yes	Yes
SNMPv2C	Yes	Yes	Yes
SNMPv3 - 3DES and AES Encryption Support	Yes	Yes	Yes
SNMPv3 (SNMP Version 3)	Yes	Yes	Yes
Source Specific Multicast (SSM)	No	Yes	Yes
Source Specific Multicast (SSM) - IGMPv3,IGMP v3lite, and URD	No	Yes	Yes
Source Specific Multicast (SSM) Mapping	No	Yes	Yes
Span Enhancement: Packet Type and Address Type Filtering	Yes	Yes	Yes
Spanning Tree Protocol (STP)	Yes	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
Spanning Tree Protocol (STP) - Backbone Fast Convergence	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Loop Guard	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Portfast	Yes	Yes	Yes
Spanning Tree Protocol (STP) - PortFast BPDU Filtering	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Portfast BPDU Guard	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Portfast Support for Trunks	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Root Guard	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Uplink Fast Convergence	Yes	Yes	Yes
Spanning Tree Protocol (STP) - Uplink Load Balancing	Yes	Yes	Yes
Spanning Tree Protocol (STP) Extension	Yes	Yes	Yes
SSO - HSRP	No	Yes	Yes
SSO - IGMP Snooping	No	Yes	Yes
Standard IP Access List Logging	Yes	Yes	Yes
Standby Supervisor Port Usage	Yes	Yes	Yes
Sticky Port Security	Yes	Yes	Yes
Sticky Port Security on Voice VLAN	Yes	Yes	Yes
Storm Control - Per-Port Multicast Suppression	Yes	Yes	Yes
STP Syslog Messages	Yes	Yes	Yes
Stub IP Multicast Routing	No	Yes	Yes
Sub-second UDLD	Yes	Yes	Yes
SVI (Switch Virtual Interface) Autostate Exclude	Yes	Yes	Yes
Switch and IP Phone Security Interaction	Yes	Yes	Yes
Switch Port Analyzer (SPAN)	Yes	Yes	Yes
Switch Port Analyzer (SPAN) - CPU Source	Yes	Yes	Yes
Syslog over IPV6	Yes	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
System Logging - EAL4 Certification Enhancements	No	Yes	Yes
TACACS SENDAUTH function	Yes	Yes	Yes
TACACS Single Connection	Yes	Yes	Yes
TACACS+	Yes	Yes	Yes
TACACS+ and Radius for IPv6-	Yes	Yes	Yes
TCAM4 - Dynamic Multi-Protocol	Yes	Yes	Yes
TCAM4 - Service-Aware Resource Allocation	Yes	Yes	Yes
Time Domain Reflectometry (TDR)[3]	No	Yes	Yes
Time-Based Access Lists	Yes	Yes	Yes
Time-Based Access Lists Using Time Ranges (ACL)	Yes	Yes	Yes
Trusted boundary (extended trust for CDP devices)	Yes	Yes	Yes
TrustSec: IEEE 802.1ae MACSec Layer 2 encryption	No	Yes	Yes
TrustSec: IEEE 802.1ae MACSec encryption on user facing ports	No	Yes	Yes
TrustSec: IEEE 802.1ae MACSec encryption on user facing ports SSO	No	Yes	Yes
TrustSec: IEEE 802.1ae MACSec encryption between switch-to-switch links using Cisco SAP (Security Association Protocol)	No	Yes	Yes
TrustSec SGT Exchange Protocol (SXP) IPv4	No	Yes	Yes
UDI - Unique Device Identifier	Yes	Yes	Yes
Uni-Directional Link Routing (UDLR)	No	Yes	Yes
Unicast Mac Filtering	Yes	Yes	Yes
Unicast Reverse Path Forwarding (uRPF)	No	Yes	Yes
Unidirectional Ethernet	Yes	Yes	Yes
UniDirectional Link Detection (UDLD)	Yes	Yes	Yes
Virtual Router Redundancy Protocol (VRRP)	No	Yes	Yes
Virtual Trunking Protocol (VTP) - Pruning	Yes	Yes	Yes

Table 1 LAN Base/IP Base/Enterprise Services Image Support on Cisco Catalyst 4500E Supervisor Engine 8-E

Feature	LAN Base	IP Base	Enterprise Services
VLAN Access Control List (VACL)	Yes	Yes	Yes
VLAN MAC Address Filtering	Yes	Yes	Yes
VLAN Mapping (VLAN Translation)	No	Yes	Yes
VRF-aware TACACS+	No	No	Yes
VTP (Virtual Trunking Protocol) Version 2	Yes	Yes	Yes
VTP Version 3	Yes	Yes	Yes
WCCP Version 2	No	Yes	Yes
Web Authentication Proxy	Yes	Yes	Yes
Webauth Enhancements	Yes	Yes	Yes
Wireshark-based Ethernet Analyzer	No	Yes	Yes
XML-PI	Yes	Yes	Yes

1. EEE 802.1t—An IEEE amendment to IEEE 802.1D that includes extended system ID, long path cost, and PortFast.
2. IP Base supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 200 dynamically learned routes.
3. TDR is not supported on 46xx linecards.

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

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

Features Not Supported on the Cisco Catalyst 4500E Series Switch, IOS Release XE 3.3.0XO

The following features are not supported on a Catalyst 4500E Series Switch with Supervisor Engine 8-E:

- Bi-Directional Forwarding Detection (BFD) Support for Routing Protocols—Provides IPv4 and IPv6 based BFD support for static routes and for dynamic routing protocols encompassing BGP, EIGRP and OSPF.
- CISCO-IETF-IP-FORWARD-MIB
- CISCO-IETF-IP-MIB
- High Speed Network Troubleshooting with Wireshark—Enables the 4500-X to now touch 0.5Gbps leading to high speed network troubleshooting and analysis.
- Lower Total Cost of Ownership and Ease of Use
  - Smart Install with Configuration-only Deployment and Smooth Upgrade
  - Other:

    Cisco OnPlus™ Service Network Agent

Different Organizations across the world have standards for compliance - some related to security, some related to IPv6 and so on (like USGv6, JITC, Common Criteria, and FIPS140).

Flexible NetFlow IPFIX (an IETF standard based on NetFlow v9) Export Format feature

Flexible Netflow Enhancements

key field supports Ethertype

non-key field supports Username, Device Type, Application Id, and Power Reading

Support for EIGRP Wide Metrics

- Multicast VLAN Registration (MVR) for Catalyst 4500E
- Security:
  - IPv6 First Hop Security (FHS):

    Source Guard

    DHCPv6 LDRA

    RA Throttler

    Neighbor Discovery (ND) Multicast Suppress
  - Trustsec Support and Enhancements:

    SGT/ SGACL

    Cisco TrustSec VLAN to SGT mapping: to co-relate source SGT with source VLAN in VLAN based environments

    IP address to SGT mapping: to co-relate source SGT with source IP address enforcing appropriate SGACL

    Port to SGT mapping: tag all traffic from a specific interface/ port

    Configurable username and password for MAB: to permit easy interoperability with RADIUS Servers/ MAC databases
- Virtual Switching Systems (VSS)
- VRF-lite support for IPv6—Expands VRF-lite support from IPv4 to IPv6, extending VRF-lite for OSPF, BGP and EIGRP.
- Zero Configuration Networking & Cisco Service Discovery Gateway

Orderable Product Numbers

Table 2 Cisco IOS XE Release 3.3.0XO Product Numbers and Images for the Catalyst 4500E Series Switch

Product Number	Description
WS-X45-SUP8-E	Cisco Catalyst 4500E Series Unified Access Supervisor, 928 Gbps
WS-C4510RE-S8+96V+	4510R+E Chassis, two WS-X4748-RJ-45V+E, Supervisor 8-E
S845EU-33-1511XO	Cisco Catalyst 4500 Supervisor Engine 8-E Cisco IOS® XE Software Release 3.3.0XO noncrypto universal image

Table 2 Cisco IOS XE Release 3.3.0XO Product Numbers and Images for the Catalyst 4500E Series Switch

Product Number	Description
S845EUK9-33-1511XO	Cisco Catalyst 4500 Supervisor Engine 8-E Cisco IOS XE Software Release 3.3.0XO crypto universal
S845EULPE-33-1511XO	Cisco Catalyst 4500 Supervisor Engine 8-E Cisco IOS XE Software Release 3.3.0XO universal LPE image
C4500E-LB	LAN BASE software license
C4500E-IPB	IP BASE software license
C4500E-LIC=	Base product ID for paper delivered software upgrade licenses
C4500E-LB-IPB	LAN BASE to IP BASE upgrade license (paper delivery)
C4500E-LB-ES	LAN BASE to Enterprise Services upgrade license (paper delivery)
C4500E-LIC-PAK	Base product ID for paper delivered software licenses for spare Supervisor Engine 8-E
C4500E-IP-ES-S	IP BASE to Enterprise Services upgrade license for spare Supervisor Engine 8-E (paper delivery)
C4500E-IPB-S	IP BASE software license for spare Supervisor Engine 8-E (paper delivery)
L-C4500-LIC=	Base product ID for electronically delivered software upgrade licenses
L-C4500E-LB-IP	LAN BASE to IP BASE upgrade license (electronically delivered)
L-C4500E-IP-ES	IP BASE to Enterprise Services upgrade license (electronically delivered)
L-C4500E-LB-ES	LAN BASE to Enterprise Services upgrade license (electronically delivered)
SD-X45-2GB-E	Cisco Catalyst 4500 2 GB SD Memory Card for Supervisor 8-E

Support

Support for Cisco IOS XE Release 3.3.0XO 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 series switches, visit the following URL:

http://www.cisco.com/go/cat4500/docs

System Requirements

This section describes the system requirements:

Supported Hardware on the Catalyst 4500E Series Switch

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

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

Table 3 lists the hardware supported on the Catalyst 4500E Series Switch.

Table 3 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 8-E

Product Number (append with "=" for spares)	**Product Description**
10 Gigabit Ethernet Switching Modules	
WS-X4712-SFP+E	12-port 10 Gigabit Ethernet (SFP+) line card
WS-X4606-X2-E	6-port X2 line card
Gigabit Ethernet Switching Modules	
WS-X4306-GB	6-port 1000BASE-X (GBIC) Gigabit Ethernet switching module
WS-X4412-2GB-T	12-port 1000BASE-T Gigabit Ethernet and 2-GBIC ports switching module
WS-X4448-GB-LX	48-port 1000BASE-LX (small form-factor pluggable) Gigabit Ethernet fiber optic interface switching module
WS-X4448-GB-SFP	48-port 1000BASE-X (small form-factor pluggable) module
WS-X4548-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet module
WS-X4548-GB-RJ45V	48-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af
WS-X4548-RJ45V+	48-port 10/100/1000 Premium PoE line card
WS-X4612-SFP-E	12-port 1000BASE-X (small form factor pluggable) module with jumbo frame support
WS-X4624-SFP-E	Non-blocking 24-port 1000BASEX (small form factor pluggable) module
WS-X4640-CSFP-E	80 ports with Gigabit compact SFP (4:1 oversubscribed); 40 modules of Gigabit SFP line card (1000BaseX), providing 24 gigabits per-slot capacity (SFP optional) (2:1 oversubscribed) **Note** WS-X4640-CSFP-E is not supported in a 10-slot chassis.
WS-X4648-RJ45-E	48 port 10/100/1000BT with 2 to 1 oversubscription and jumbo frame support
WS-X4648-RJ45V-E	48 port 10/100/1000 Mb with 2 to 1 oversubscription PoE 802.3af providing up to 20 Watts power/port
WS-X4648-RJ45V+E	48 port 10/100/1000 Mb with 2 to 1 oversubscription PoE 802.3at providing up to 30 Watts power/port
WS-X4748-RJ45V+E	48-port 10/100/1000 line card nonblocking PoE 802.3at providing up to 30 Watts power/port
WS-X4748-UPOE+E	48-port 10/100/1000 line card nonblocking PoE 802.3at and 60 watt UPoE PoE linecard with Ethernet Energy Efficient feature.

Table 3 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 8-E

Product Number (append with "=" for spares)	**Product Description**
WS-X4748-RJ45-E	48-port 10/100/1000 nonblocking line card with the Ethernet Energy Efficient feature
Fast Ethernet Switching Modules	
WS-X4148-FX-MT	48-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module
WS-X4148-FE-LX-MT	48-port 100BASE-LX10 Fast Ethernet MT-RJ single-mode fiber switching module
WS-X4248-FE-SFP	48-port 100BASE-X SFP switching module
WS-U4504-FX-MT	4-port 100BASE-FX (MT-RF) uplink daughter card
Ethernet/Fast Ethernet (10/100) Switching Modules	
WS-X4148-RJ	48-port 10/100 RJ-45 switching module
WS-X4148-RJ21	48-port 10/100 4xRJ-21 (telco connector) switching module
WS-X4148-RJ45V	48-port Pre-standard PoE 10/100BASE-T switching module
WS-X4232-GB-RJ	32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet switching module
WS-X4248-RJ45V	48-port 10/100BASE-T RJ-45 Cisco Catalyst 4500 series PoE 802.3af
WS-X4232-RJ-XX	32-port 10/100 Fast Ethernet RJ-45 modular uplink switching module
Small Form-Factor Pluggable 100 Megabit Ethernet Modules	
GLC-FE-100LX	100BASE-LX, 1310 nm wavelength, 10 km over SMF
GLC-FE-100BX-D	100BASE-BX10-D, 1550 nm TX/1310 nm RX wavelength
GLC-FE-100BX-U	100BASE-BX10-U, 1310 nm TX/1550 nm RX wavelength
GLC-FE-100EX	100BASE-EX for Fast Ethernet SFP Ports
GLC-FE-100ZX	100BASE-ZX for Fast Ethernet SFP Ports
GLC-FE-100FX	100BASE-FX SFP for Fast Ethernet SFP ports
GLC-GE-100FX	100BASE-FX SFP for Gigabit Ethernet SFP ports
GLC-EX-SMD	1000BASE-EX GE SFP ports
Small Form-Factor Pluggable Gigabit Ethernet Modules	
GLC-BX-D	1000BASE-BX10-D small form-factor pluggable module For DOM support, see Table 6 on page 30.
GLC-BX-U	1000BASE-BX10-U small form-factor pluggable module For DOM support, see Table 6 on page 30.bv
GLC-SX-MM	1000BASE-SX small form-factor pluggable module
GLC-SX-MMD	1000BASE-SX small form-factor pluggable module with DOM support
GLC-LH-SM	1000BASE-LX/LH small form-factor pluggable module
GLC-LH-SMD	1000BASE-LX/LH small form-factor pluggable module with DOM support
GLC-ZX-SM	1000BASE-ZX small form-factor pluggable module
GLC-T	1000BASE-T small form-factor pluggable module

Table 3 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 8-E

Product Number (append with "=" for spares)	**Product Description**
CWDM-SFP-xxxx	CWDM small form-factor pluggable module (See Table 4 on page 29 for a list of supported wavelengths.) For DOM support, see Table 6 on page 30.
10 Gigabit Ethernet X2 Pluggable Modules	
X2-10GB-LR	10GBASE-LR X2 transceiver module for SMF, 1310-nm wavelength, SC duplex connector
X2-10GB-ER	10GBASE-ER X2 transceiver module for SMF, 1550-nm wavelength, SC duplex connector
X2-10GB-CX4	10GBASE-CX4 X2 transceiver module for CX4 cable, copper, Infiniband 4X connector
X2-10GB-LX4	10GBASE-LX4 X2 transceiver module for MMF, 1310-nm wavelength, SC duplex connector
X2-10GB-LRM	10GBASE-LRM X2 transceiver module for MMF, 1310-nm wavelength, SC duplex connector
X2-10GB-SR	10GBASE-SR X2 transceiver module for MMF, 850-nm wavelength, SC duplex connector
X2-10GB-ZR	10GBASE-ZR X2 transceiver module for SMF, 1550 nm wavelength up to 80 km. DOM is not supported.
X2-10GB-DWDM	10GBASE-ZR X2 transceiver module for SMF, 32 nontunable ITU 100-GHz wavelengths up to 80 km are supported. DOM is supported. Dual SC/PC connectors are supported.
CVR-X2-SFP10G	Hot-swappable input/output (I/O) converter module that fits into a 10-Gigabit Ethernet X2 slot on a switch or line card module. Hosts one 10-Gigabit Ethernet SFP+ transceiver module.
SFP+ Modules	
SFP-10G-SR	Cisco 10GBASE-SR SFP+ Module for MMF
SFP-10G-LR	Cisco 10GBASE-LR SFP+ Module for SMF
SFP-10G-LRM	Cisco 10GBASE-LRM SFP+ Module for MMF
SFP-H10GB-CU1M	10GBASE-CU SFP+ Cable 1 Meter
SFP-H10GB-CU3M	10GBASE-CU SFP+ Cable 3 Meter
SFP-H10GB-CU5M	10GBASE-CU SFP+ Cable 5 Meter
SFP-10G-ER	Cisco 10GBASE-ER SFP+ Module for SMF
SFP-10G-ZR	Cisco 10GBASE-ZR SFP+ Module for SMF
Gigabit Interface Converter	
WS-G5483=	1000BASE-T GBIC
WS-G5484	1000BASE-SX short wavelength GBIC (multimode only)
WS-G5486	1000BASE-LX/LH long-haul GBIC (single mode or multimode)
WS-G5487	1000BASE-ZX extended reach GBIC (single-handed)
CWDM-GBIC-xxxx	CWDM gigabit interface converter (See Table 4 on page 29 for a list of supported wavelengths.)
DWDM-GBIC-xx.yy	Dense Wavelength-Division Multiplexing ITU 100-Ghz grid 15xx.yy nm GBIC. For DOM support, see Table 6 on page 30.
WDM-GBIC-REC	Receive-only 1000BASE-WDM GBIC
Other Modules	
MEM-X45-2GB-E	SD Card, 2G

Table 3 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 8-E

Product Number (append with "=" for spares)	**Product Description**
PWR-C45-1000AC	Catalyst 4500 series switch 1000 Watt AC power supply for chassis 4503, 4506, and 4507R (data only)
PWR-C45-1400DC	Catalyst 4500 series switch 1400 Watt DC triple input power supply (data-only)
PWR-C45-1400DC-P	Catalyst 4500 series switch 1400 Watt DC power supply with integrated PEM
PWR-C45-1400AC	Catalyst 4500 series switch 1400 Watt AC power supply (data-only)
PWR-C45-1300ACV	Catalyst 4500 series switch 1300 Watt AC power supply with integrated voice for chassis 4503, 4506, and 4507R
PWR-C45-2800ACV	Catalyst 4500 series switch 2800 Watt AC power supply with integrated voice (data and PoE) for chassis 4503, 4506, and 4507R
PWR-C45-4200ACV	Catalyst 4500 series switch 4200 Watt AC dual input power supply with integrated voice (data and PoE)
WS-P4502-1PSU	Catalyst 4500 series switch auxiliary power shelf (25-slot), including one PWR-4502
PWR-4502	Catalyst 4500 series switch auxiliary power shelf redundant power supply
PWR-C45-6000ACV	Catalyst 4500 Series Switch 6000 W AC power supply

Table 4 briefly describes the supported CWDM wavelengths in the Catalyst 4500E Series Switch.

Table 5 briefly describes the supported DWDM wavelengths in the Catalyst 4500E Series Switch.

Table 4 CWDM GBIC and SFP Supported Wavelengths on Cisco Catalyst 4500E Supervisor Engine 8-E

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

Table 5 DWDM SFP Supported Wavelengths on Cisco Catalyst 4500E Supervisor Engine 8-E

Product Number (append with "=" for spares)	**Product Description**
DWDM-SFP-6061=	Cisco 1000BASE-DWDM SFP 1560.61 nm
DWDM-SFP-5979=	Cisco 1000BASE-DWDM SFP 1559.79 nm
DWDM-SFP-5898=	Cisco 1000BASE-DWDM SFP 1558.98 nm

Table 5 DWDM SFP Supported Wavelengths on Cisco Catalyst 4500E Supervisor Engine 8-E

Product Number (append with "=" for spares)	**Product Description**
DWDM-SFP-5817=	Cisco 1000BASE-DWDM SFP 1558.17 nm
DWDM-SFP-5655=	Cisco 1000BASE-DWDM SFP 1556.55 nm
DWDM-SFP-5575=	Cisco 1000BASE-DWDM SFP 1555.75 nm
DWDM-SFP-5413=	Cisco 1000BASE-DWDM SFP 1554.13 nm
DWDM-SFP-5494=	Cisco 1000BASE-DWDM SFP 1554.94 nm
DWDM-SFP-5252=	Cisco 1000BASE-DWDM SFP 1552.52 nm
DWDM-SFP-5172=	Cisco 1000BASE-DWDM SFP 1551.72 nm
DWDM-SFP-5092=	Cisco 1000BASE-DWDM SFP 1550.92 nm
DWDM-SFP-5012=	Cisco 1000BASE-DWDM SFP 1550.12 nm
DWDM-SFP-4851=	Cisco 1000BASE-DWDM SFP 1548.51 nm
DWDM-SFP-4772=	Cisco 1000BASE-DWDM SFP 1547.72 nm
DWDM-SFP-4692=	Cisco 1000BASE-DWDM SFP 1546.92 nm
DWDM-SFP-4612=	Cisco 1000BASE-DWDM SFP 1546.12 nm
DWDM-SFP-4453=	Cisco 1000BASE-DWDM SFP 1544.53 nm
DWDM-SFP-4373=	Cisco 1000BASE-DWDM SFP 1543.73 nm
DWDM-SFP-4694=	Cisco 1000BASE-DWDM SFP 1542.94 nm
DWDM-SFP-4614=	Cisco 1000BASE-DWDM SFP 1542.14 nm
DWDM-SFP-4056=	Cisco 1000BASE-DWDM SFP 1540.56 nm
DWDM-SFP-3977=	Cisco 1000BASE-DWDM SFP 1539.77 nm
DWDM-SFP-3898=	Cisco 1000BASE-DWDM SFP 1539.98 nm
DWDM-SFP-3819=	Cisco 1000BASE-DWDM SFP 1538.19 nm
DWDM-SFP-3661=	Cisco 1000BASE-DWDM SFP 1536.61 nm
DWDM-SFP-3582=	Cisco 1000BASE-DWDM SFP 1535.82 nm
DWDM-SFP-3504=	Cisco 1000BASE-DWDM SFP 1535.04 nm
DWDM-SFP-3425=	Cisco 1000BASE-DWDM SFP 1534.25 nm
DWDM-SFP-3268=	Cisco 1000BASE-DWDM SFP 1532.68 nm
DWDM-SFP-3190=	Cisco 1000BASE-DWDM SFP 1531.90 nm
DWDM-SFP-3112=	Cisco 1000BASE-DWDM SFP 1531.12 nm
DWDM-SFP-3033=	Cisco 1000BASE-DWDM SFP 1530.33 nm

Table 6 briefly describes the DOM support on the Catalyst 4500E Series Switch.

Table 6 DOM Support on Cisco Catalyst 4500E Supervisor Engine 8-E

SFP	GLC-BX-D
SFP	GLC-BX-U

Table 6 DOM Support on Cisco Catalyst 4500E Supervisor Engine 8-E

SFP	GLC-FX-SMD
SFP	GLC-SX-MMD
SFP	GLC-LH-SMD
SFP	CWDM
SFP	DWDM (24 wavelengths)
X2	X2-10GB-LR
X2	X2-10GB-SR
X2	X2-10GB-ER
X2	X2-10GB-LRM
X2	X2-10GB-DWDM
X2	X2-10GB-ZR
SFP+	SFP-10G-ER
SFP+	SFP-10G-LR
SFP+	SFP-10G-LRM
SFP+	SFP-10G-SR
SFP+	SFP-10G-ZR

Supported E Series Hardware on Cisco IOS XE Release 3.3.0XO

A brief list of primary E-Series hardware supported by Cisco IOS XE Release 3.3.0XO is shown in Table 7.

Table 7 Supported E-Series Hardware

Product Number	Description
WS-C4503-E	Cisco Catalyst 4500E Series 3-Slot Chassis • Fan tray • No Power Supply • Slot 1 only
WS-C4506-E	Cisco Catalyst 4500E Series 6-Slot Chassis • Fan tray • No Power Supply • Slot 1 only

Table 7 Supported E-Series Hardware

Product Number	Description
WS-C4507R+E	Cisco Catalyst 4500E Series 7-Slot 48 GB-ready Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 3 and/or 4; the backplane will enforce this restriction.
WS-C4510R+E	Cisco Catalyst 4500E Series 10-Slot 48 GB-ready Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • Supervisor engines must sit in slots 5 and/or 6; the backplane will enforce this restriction. • Last two slots can only support 47xx linecards; older 46xx cards are not supported.

Cisco IOS XE to Cisco IOS Version Number Mapping

As Table 8 shows, each version of Cisco IOS XE has an associated Cisco IOS version:

Table 8 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOS Version
03.3.0XO	15.1(1)XO
03.3.1XO	15.1(1)XO1
03.4.0SG	15.1(2)SG
03.5.0E	15.2(1)E

Limitations and Restrictions

These sections list the limitations and restrictions for the current release of Cisco IOS software on the Catalyst 4500E series switch.

- For the 10-slot chassis, (C4510R+E), slot 10 can only support 47xx linecards; older 46xx are not supported.
- Starting with Release IOS XE 3.3.0SG, the seven RP restriction was removed.
- More than 16K QoS policies can be configured in software. Only the first 16K are installed in hardware.
- Adjacency learning (through ARP response frames) is restricted to roughly 1000 new adjacencies per second, depending on CPU utilization. This should only impact large networks on the first bootup. After adjacencies are learned they are installed in hardware.

- Multicast fastdrop entries are not created when RPF failure occurs with IPv6 multicast traffic. In a topology where reverse path check failure occurs with IPv6 multicast, this may cause high CPU utilization on the switch.
- The SNMP ceImageFeature object returns a similar feature list for all the three license levels (LAN Base, IP Base, and EntServices). Although the activated feature set for a universal image varies based on the installed feature license, the value displayed by this object is fixed and is not based on the feature license level.
- Standard TFTP implementation limits the maximum size of a file that can be transferred to 32 MB. If ROMMON is used to boot an IOS image that is larger than 32 MB, the TFTP transfer fails at the 65,*xxx* datagram.

  TFTP numbers its datagrams with a 16 bit field, resulting in a maximum of 65,536 datagrams. Because each TFTP datagram is 512 bytes long, the maximum transferable file is 65536 x 512 = 32 MB. If both the TFTP client (ROMMON) and the TFTP server support block number wraparound, no size limitation exists.

  Cisco has modified the TFTP client to support block number wraparound. So, if you encounter a transfer failure, use a TFTP server that supports TFTP block number wraparound. Because most implementations of TFTP support block number wraparound, updating the TFTP daemon should fix the issue.
- A XML-PI specification file entry does not return the desired CLI output.

  The outputs of certain commands, such as **show ip route** and **show access-lists**, contain non-deterministic text. While the output is easily understood, the output text does not contain strings that are consistently output. A general purpose specification file entry is unable to parse all possible output.

  Workaround (1):

  While a general purpose specification file entry may not be possible, a specification file entry might be created that returns the desired text by searching for text that is guaranteed to be in the output. If a string is guaranteed to be in the output, it can be used for parsing.

  For example, the output of the **show ip access-lists SecWiz_Gi3_17_out_ip** command is this:

```
Extended IP access list SecWiz_Gi3_17_out_ip
    10 deny ip 76.0.0.0 0.255.255.255 host 65.65.66.67
    20 deny ip 76.0.0.0 0.255.255.255 host 44.45.46.47
    30 permit ip 76.0.0.0 0.255.255.255 host 55.56.57.57
```

  The first line is easily parsed because access list is guaranteed to be in the output:

```
<Property name="access list" alias="Name" distance="1.0" length="-1" type="String"
/>
```

  The remaining lines all contain the term host. As a result, the specification file may report the desired values by specifying that string. For example, this line

```
<Property name="host" alias="rule" distance="s.1" length="1" type="String" />
```

  will produce the following for the first and second rules

```
<rule>
    deny
</rule>
```

  and the following for the third statement

```
<rule>
    permit
<rule>
```

Workaround (2):

Request the output of the **show running-config** command using NETCONF and parse that output for the desired strings. This is useful when the desired lines contain nothing in common. For example, the rules in this access list do not contain a common string and the order (three permits, then a deny, then another permit), prevent the spec file entry from using permit as a search string, as in the following example:

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

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

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

CSCtg93278

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

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

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

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

  Workarounds:

  - Decrease the number of monitors.
  - Attach the same monitor to multiple targets. CSCti43798

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

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

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

  - At least 10K groups and roughly 20K mroutes exist.
  - IGMP joins with source traffic transit to all the multicast groups.

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

  Workaround: None. CSCti20312

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

- 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.

- With Cisco IOS Release XE 3.2.1SG, **memory** configuration is enabled:

  ```
  Switch(config)# memory ?
    chunk    chunk related configuration
    free     free memory low water mark
    record   configure memory event/traceback recording options
    reserve  reserve memory
    sanity   Enable memory sanity
  ```

  This configuration had been removed erroneously in a prior release.

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

  Workaround: None. CSCtr51014

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

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

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

  Workaround: Select an alternate destination or source port. CSCty05405

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

  Workaround: None. CSCty79236

- When sup1 is in ROMMON and sup2 is in IOS, only sup2 can read the SEEPROM contents of the following chassis components:
  - chassis
  - fan-tray
  - clock-module
  - power-supplies
  - mux-buffer for each linecard slot
  - linecards

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

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

- On the following linecard:
  - 10/100/1000BaseT Premium POE E Series WS-X4648-RJ45V+E (JAE1348OY52)

  the following restrictions apply:
  - Sub-interfaces are not supported.
  - Port-channel members do not support multiple classification criteria for a QoS policy.
  - CEF is disabled automatically when uRFP is enabled and TCAM is fully utilized.
- 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.

  Workaround: During IPv6 access-list configuration, configure at least one IPv6 ACE before the "hardware statistics" statement. CSCuc53234
- With IOS Release XE 3.3.0X0, ROMMON supports the Fa1 management interface at 10/100/1000Mbps full duplex mode only; 10/100/1000Mbps half-duplex is not supported. This prevents the FA1 management interface from operating when connected to a half-duplex hub.
- Supervisor Engine 8-E does not support USB port.
- Memory allocation failures can occur if more than 16K IPv6 multicast snooping entries are present.

  Workaround: None. CSCuc77376
- The following messages are seen during boot up after POST check.

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

Image load status: 0x00000000
#####
Snowtrooper 220 controller 0x0430006E..0x044E161D Size:0x0057B4C5 Program Done!
#########################
[ 6642.974087] pci 0000:00:00.0: ignoring class b20 (doesn't match header type 01)
Starting System Services
Calculating module dependencies ...
Loading rtc-ds1307
RTNETLINK answers: Invalid argument
No Mountpoints DefinedJan 17 09:48:14 %IOSXE-3-PLATFORM: process sshd[5241]: error:
Bind to port

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

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

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

  Workaround: None. CSCue15724/CSCui56436

Caveats

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

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

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

Open Caveats for Cisco IOS XE Release 3.3.2XO

This section lists the open caveats for Cisco IOS XE Release 3.3.2XO:

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

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

  Workaround: None. CSCts20229

- When you 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

- A device in a guest VLAN that is connected behind a phone that is 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 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

- IPv6 access-list counters do not increment when a policy-map associated with a class-map that matches a v6 ACL is applied to a physical interface and matching traffic is sent.

```
juhani07-a#sh ipv6 access-list v6acl
IPv6 access list v6acl
    permit ipv6 host 2003::2 any (1000 matches) sequence 10   --- only 1000 matched
although 2000 matching pkts sent
    permit ipv6 host 2004::2 any sequence 20
```

  Workaround: None CSCug54690

- If you configure a Qos srTCM policer with actions (traffic conform, traffic exceed, and traffic violated), the marking action for exceed traffic remains inactive.

Workaround: Configure a policer with only conform-action and exceed-action and not with violate-action. CSCug49778.

- When a linecard is reset on a switch using multicast, a message like the following map appear:

  ```
  PIM_REG_TUN-3-UNNUM_ERR: STANDBY
  ```

  This error is informational only.

  Workaround: None. CSCug19842

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

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

  CSCue47944

- The IOS Supplicant fails authentication when using PEAPv1 or MSChap to ACS 5.

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

- Immediately following an SSO, the following error message may be logged by the new active route processor:

  ```
  %MRIB_PROXY-2-MRIB_RP_FAILED_LC_PORT_OPEN: RP failed in opening linecard port info for
  distributed mode, slot = 3.  MRIB updates will not be distributed to this LC.
  ```

  The error message is information only.

  Workaround: None. CSCuc72249

- 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 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.

  The impact of stale dynamic access lists is to monitor unwanted traffic.

  Workarounds:

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

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

  Workaround: None. CSCtu37959

- 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

- 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

- On second switchover, MKA sessions go down and never recover.

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

  Applying the workaround preemptively (i.e., entering **shut** then **no shut** on the interfaces after first switchover) prevents a failure on the subsequent switchover. CSCui49000

- On second switchover, MKA sessions go down and never recover.

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

  Applying the workaround preemptively (i.e., entering **shut** then **no shut** on the interfaces after first switchover) prevents a failure on the subsequent switchover. CSCui49000

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

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

  CSCto27085

- 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

- 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

- A traceback is seen after two switchovers with Rev 2 Boards.

```
MINGLA# show mod
Chassis Type : WS-C4507R+E

Power consumed by backplane : 40 Watts

Mod Ports Card Type                              Model              Serial No.
---+-----+--------------------------------------+------------------+-----------
 1    48  10/100/1000BaseT Premium POE E Series  WS-X4748-RJ45V+E   CAT1340L01H
 2    48  10/100/1000BaseT (RJ45)                WS-X4648-RJ45-E    JAE1345N81O
 3     8  Sup 8-E 10GE (SFP+), 1000BaseX (SFP)   WS-X45-SUP8-E      CAT1720L1W1
 4     8  Sup 8-E 10GE (SFP+), 1000BaseX (SFP)   WS-X45-SUP8-E      CAT1720L1WN
 5    48  1000BaseX SFP                          WS-X4448-GB-SFP    JAB090504ED
 7    48  10/100/1000BaseT UPOE E Series         WS-X4748-UPOE+E    CAT1615L118

 M MAC addresses                   Hw  Fw           Sw               Status
--+--------------------------------+---+------------+----------------+---------
 1 0026.9927.c340 to 0026.9927.c36f 0.2                               Ok
 2 0024.1447.0512 to 0024.1447.0541 1.0                               Ok
 3 acf2.c5df.8500 to acf2.c5df.8507 0.4 15.1(1r)SG(0 03.05.00.EX0.146 Ok
 4 acf2.c5df.8508 to acf2.c5df.850f 0.4 15.1(1r)SG(0 03.05.00.EX0.146 Ok
 5 0012.7f9a.baf0 to 0012.7f9a.bb1f 1.0                               Ok
 7 5057.a886.d670 to 5057.a886.d69f 1.1                               Ok
```

```
Mod  Redundancy role     Operating mode      Redundancy status
----+-------------------+-------------------+-----------------------------------
 3   Standby Supervisor  SSO                 Standby hot
 4   Active Supervisor   SSO                 Active
```

Workaround: None. CSCui25812

- On IOS Release 15.2(1)E, the DUT MAC learn rate (4700 MAC sec) is lower than the rate (8000 MAC/sec) on IOS Release 3.4.0SG. When the **macro auto monitor** command is disabled on IOS Release 15.2(1)E, the rate is 13800 MAC/sec.

  Workaround: None. CSCui07503

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

  Workaround: None. CSCth42248

Resolved Caveats for Cisco IOS XE Release 3.3.2XO

This section lists the resolved caveats for Cisco IOS XE Release 3.3.2XO:

- WS-X4248 or WS-X4548- PoE modules reset PoE causing all connected PDs to lose power precipitating an outage. The following error log is observed:

  *Feb 4 10:05:46.648: %C4K_CHASSIS-5-PORTSPOERESTARTED: Poe restarted for interfaces on slot 5 (count=1)

  Workaround: None. CSCun21714

- If a GRE tunnel is configured with ip unnumbered and you write this configuration, after reloading the system, the FIA table is not reloaded (i.e., all packets for that tunnel are dropped under "UnconfiguredIpv4Fia").

  Workaround: Unconfigure the reconfigure the **ip unnumbered** command. CSCtb14871

- IP DHCP Snooping bindings fail on first attempt.

  Workaround: Issue either **sh run** or **write memory**. CSCui35423

- When Performance Monitor feature is configured with threshold-crossing-alarms, the SNMP query FlowMetrics,FlowMonitor,Alarm returns the wrong values. Note the following MIBs:

  ```
  cfmConditionsProfile
  cfmAlarmHistoryConditionsProfile
  cfmFlowMetricConditionsProfile
  cfmFlowMonitorConditionsProfile
  ```

  Workaround None. CSCuj48676

- When you connect GLC-GE-100FX in WS-X4624-SFP-E, WS-X4640-CSFP-E or WS-X4612-SFP-E, the link doesn't come up.

  GLC-GE-100FX was tested with WS-X4624-SFP-E(HW 1.2(VID V02) and HW 2.0(VID V03)), the problem happened on GLC-GE-100FX V02 only. There was no problem with GLC-GE-100FX V01.

  Workaround: None. CSCui23911

- "ffm" progressively takes up more memory while free memory depletes by a similar amount.

  This issue is triggered by one of the following:

  – consistent rapid flapping of mroute(s)

  - constant traffic toward a group on a VLAN where SVI is configured with PIM sparse mode but an RP is disallowed [for the group]

  Workarounds:

  - For flapping mroutes, find the source of the flapping mroute and prevent it.
  - For a missing RP scenario, either turn off PIM on the VLAN or allow the multicast group associate with an RP. CSCul44174

- If the session limit is exceeded for one flow, the **show profile device** command displays "empty:"

```
Newton# show profile flow
Source-IP       sPort Dest-IP         dPort pro I/F      Media-proxy Services profile
192.168.0.20    6840  197.168.0.2     3354  UDP Gi1/0/7  Pelco

Newton# show profile device
MAC Address     Interface    Device class            Device Model            Device
Vendor
==============  ==========   =============           ============
==============
================================================================================
=========
```

  Workaround: None. CSCul98277

- A switch crashes reliably when you issue the following command (under a VLAN) to enable unicast RPF:

```
ip verify unicast source reachable-via rx allow-default
```

  Workaround: None. CSCum90900

- After every reboot, the SNMPv2 configuration is lost; it is present in the startup-config but not in the running config. The config doesn't work after reboot:

```
snmp-server group S-GROUP-RO-GENERAL v2c read S-VIEW-GENERAL access
ACL-4-mgmtVrf-SNMP-2-RO
```

  With a different community or without **snmp-server host 192.168.131.13 vrf mgmtVrf version 2c**, the config line remains intact.

  Workaround: Re-apply this configuration. CSCsh92025

- A switch running cat4500e-universalk9.SPA.03.04.00.SG.151-2.SG.bin that points to an NTP server will observe forward clock shifting although NTP status shows that the sync is working.

  Removing or adding the NTP configuration doesn't fix the issue.

  In the following example, **show clock** is executed on ASR, then on a Catalyst 4500 switch. Notice that the Catalyst 4500 switch is nearly eight second behind:

```
ASR# sh clock
19:12:16.105 EDT Fri May 3 2013<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
4500# sh clock
19:12:08.615 EDT Fri May 3 2013<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

  Workaround: None. CSCug75425

- A PoE device connected to a interface on module WS-X4748-UPOE+E with WS-X45-SUP7-E will not power UP. The interface remains down or unconnected.

  Workarounds:

  - Run a TDR test on the port:

    test cable-diagnostics tdr interface <int> CSCui45222

- A standby switch in VSS (or a redundant supervisor engine outside VSS) reboots due to config-sync failure when moving VLAN names:

  Old:

```
 vlan 1022
   name NP-B_INet-In-EDGE
 vlan 1024
   name NP-A_WAN-6509
```

  New: (VLAN 1024 is renamed with the old name for VLAN 1022)

```
conf t
 vlan 1022
   name NP-B_INet-In-EDGE-
  !
  vlan 1024
   name NP-B_INet-In-EDGE


*Sep 24 11:35:52.293: %SYS-5-CONFIG_I: Configured from console by console
*Sep 24 11:36:09.421: Config Sync: Line-by-Line sync verifying failure on command:
     name NP-B_INet-In-EDGE
due to parser return error
*Sep 24 11:36:09.453: %RF-5-RF_RELOAD: Peer reload. Reason: Configuration
mismaCSCuj42720
```

  Workaround: Exit the VLAN config mode before changing the second VLAN name. CSCuj42720

- On executing the **show platform chassis poe** command, the switch crashes.

  Workaround: None. CSCul71294

- CISCO-FLASH-MIB returns only data for cat4000_flash partition for ciscoFlashFiles OID

```
% snmpwalk -v2c -c public FAMRIR 1.3.6.1.4.1.9.9.10.1.1.4.2
SNMPv2-SMI::enterprises.9.9.10.1.1.4.2.1.1.2.1.1.1 = Gauge32: 1576
SNMPv2-SMI::enterprises.9.9.10.1.1.4.2.1.1.3.1.1.1 = STRING: "0x0"
SNMPv2-SMI::enterprises.9.9.10.1.1.4.2.1.1.4.1.1.1 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.10.1.1.4.2.1.1.5.1.1.1 = STRING: "vlan.dat"
SNMPv2-SMI::enterprises.9.9.10.1.1.4.2.1.1.6.1.1.1 = INTEGER: 1
```

  This means that NMS systems cannot gather information about files on the other partitions.

  Workaround: None. CSCul75216

- A switch may experience a low memory condition due to increased utilization under the "Chunk Manager" process.

  If performance monitoring is configured with the **service-policy type performance-monitor input/output < >** command, your will notice that the memory held by Chunk Manager / List Headers continues to grow:

```
interface GigabitEthernet0/1
 service-policy type performance-monitor input RTPMON   <<<
 service-policy type performance-monitor output RTPMON  <<<

# show proc mem sort
Processor Pool Total: 1841279968 Used:  334068580 Free: 1507211388
      I/O Pool Total:   54525952 Used:   21823488 Free:   32702464

 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   1   0 2708385168  489355988  209773704          0          0 Chunk Manager
   0   0  365726260  212948836  111164628          0          0 *Init*
   0   0 2852653512  561502116   19385844    6960999          0 *Dead*
 333   0 2033684636 1082488700    2201728          0          0 MMA MSG MCOL
```

```
# show mem all totals

Allocator PC Summary for: Processor
Displayed first 2048 Allocator PCs only

    PC          Total   Count  Name
0x073279A4  210035320   44401  List Headers   <<
0x071F0AA8   12299796     366  CFT Data Path F

Decoded PC
0x073279A4:list_create(0x7327954)+0x50
```

Workaround: None. CSCun34312

- A switch crashes when issuing the **clear ip dchp conflict *** command

  Workaround: None. CSCui87789

- A device running IOS-XE may reload unexpectedly.

  Workaround: None. CSCul36468

- If you configure dot1x for host-mode multi-host, phones that are in a voice VLAN do not acquire an IP address and are unable to be t registered to call manager

  Workaround: Change to multi-domain or single host with CDP bypass (enable cdp/lldp on the switch). CSCuo79422

- A switch crashes with Critical software exception during config push as 'Critical software exception'

  Workload: None. CSCup39712

- During an HA setup, the active supervisor engine reload does not complete within the allocated time and the following error message is displayed

  ```
  %C4K_CHASSIS-3-MODULEBRINGUPTIMEDOUT: Module 2 software bring up did not complete
  within allocated time
   %C4K_CHASSIS-3-MODULEBRINGUPTIMEDOUT: Module 1 software bring up did not complete
  within allocated time
  ```

  Workaround: None. CSCuq17614

- High CPU is observed when sending multicast traffic provided the switch is directly connected to the source and PIM SSM is configured but no receiver exists.

  Workaround: Configure control plane policy to deny Multicast SSM traffic hitting CPU.

  CSCub10733

- Non-interested multicast traffic for PIM SM is punted to CPU after an IOS upgrade to IOS 15.1(2)SG.

  Workarounds:

  1. Apply ACL on ingress interface deny the non-interested PIM SM multicast stream:

  ```
  enderman# show ip access-lists TAC
  Extended IP access list TAC
      10 deny ip host 10.1.1.3 host 239.1.1.5 (40 estimate matches)
      20 permit ip any any (42 estimate matches)
  ```

  2. Have a dummy loopback interface enabled with PIM-SM. Configure **ip igmp static-group *x.x.x.x*** on this Loopback interface (where *x.x.x.x* is non-interested multicast group ip address). CSCui64652

- When PIM is enabled on an SVI interface, multicast traffic is dropped in certain scenario where it requires Layer 2 switching (Router on which Multicast (*, G) or (S, G) entry is not present for Group).

Workaround: Disable PIM SSM on the interface. CSCum47920

- High CPU is observed with multicast SSM traffic, when the Source is directly connect to the Router.

  Moreover, mroute is improperly programmed on the switch, which is connected to multicast source.

  CSCuo06555

- Multicast (S,G) entries are not created on intermediate routers running in PIM Dense-mode.

  Workaround: None. CSCuo47803

- Non-interested multicast traffic only is punted to CPU after upgrading to IOS Release 151-2.SG

  Workarounds

  – Apply ACL on ingress interface denying the non-interested multicast stream. Below is the example.

  ```
  enderman# show ip access-lists TAC
  Extended IP access list TAC
      10 deny ip host 10.1.1.3 host 239.1.1.5 (40 estimate matches)
      20 permit ip any any (42 estimate matches)
  ```

  – Use a dummy loopback interface enabled with PIM-SM. Configure **ip igmp static-group** *x.x.x.x* on this Loopback interface (where *x.x.x.x* is the non-interested multicast group ip address).

  CSCui64652

Open Caveats for Cisco IOS XE Release 3.3.1XO

This section lists the open caveats for Cisco IOS XE Release 3.3.0XO:

- When an SNMP query includes the cpmCPUProcessHistoryTable, the query time is very slow, and CPU utilization of the os_info_p process (OS Info provider) increases substantially. The time required for a full walk 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 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 reboot a switch, the configured value of the interface MTU size for the elements of the port channel interface does not work for IPv6 traffic.

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

  CSCto27085

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

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

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

  Workaround: None. CSCto46018
- If you perform an OIR on a line card, several %C4K_RKNOVA-4-INVALIDTOKENEXPIRED messages appear in the logs.

  Workaround: None. CSCtu37959
- When you enable both Cisco TrustSec and RADIUS accounting, a disparity occurs between the RADIUS client (Cisco switch) and the RADIUS/CTS server in how the authenticator field in the header is computed for DOT1X/RADIUS accounting messages.

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

  Workaround: None. You must disable 802.1X accounting. CSCts26844
- When more than one Equal Cost Multipath (ECMP) is available on the downstream switch, and Mediatrace is invoked to provide flow statistics, the dynamic policy does not show statistics for a flow.

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

  Workaround: None. CSCts20229
- When a switchover is created on the Mediatrace responder, the dynamic access list created for a monitored flow tuple is not deleted. Although the Mediatrace initiator creates another set of dynamic access lists after the switchover, the old ones remain in the configuration.

  The impact of stale dynamic access lists is to monitor unwanted traffic.

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

  Workaround: Do not specify a "bfd" suffix with the **snmp-server host** *x.x.x.x* configuration command. CSCtx51561
- During either a system- or user-initiated reload operation, the following message is observed when the system shuts down:

  ```
  HARDWARE WATCHDOG
  ```

  This message is not observed during a system bootup.

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

- Immediately following an SSO, the following error message may be logged by the new active route processor:

```
%MRIB_PROXY-2-MRIB_RP_FAILED_LC_PORT_OPEN: RP failed in opening linecard port info for
distributed mode, slot = 3.  MRIB updates will not be distributed to this LC.
```

  The error message is information only.

  Workaround: None. CSCuc72249

- On IOS Release 15.2(1)E, the DUT MAC learn rate (4700 MAC sec) is lower than the rate (8000 MAC/sec) on IOS Release 3.4.0SG. When the **macro auto monitor** command is disabled on IOS Release 15.2(1)E, the rate is 13800 MAC/sec.

  Workaround: None. CSCui07503

- When a linecard is reset on a switch using multicast, a message like the following map appear:

```
PIM_REG_TUN-3-UNNUM_ERR: STANDBY
```

  This error is informational only.

  Workaround: None. CSCug19842

- If you configure a Qos srTCM policer with actions (traffic conform, traffic exceed, and traffic violated), the marking action for exceed traffic remains inactive.

  Workaround: Configure a policer with only conform-action and exceed-action and not with violate-action. CSCug49778.

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

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

  CSCue47944

- IPv6 access-list counters do not increment when a policy-map associated with a class-map that matches a v6 ACL is applied to a physical interface and matching traffic is sent.

```
juhani07-a#sh ipv6 access-list v6acl
IPv6 access list v6acl
    permit ipv6 host 2003::2 any (1000 matches) sequence 10   --- only 1000 matched
although 2000 matching pkts sent
    permit ipv6 host 2004::2 any sequence 20
```

  Workaround: None CSCug54690

- The IOS Supplicant fails authentication when using PEAPv1 or MSChap to ACS 5.

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

- On second switchover, MKA sessions go down and never recover.

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

  Applying the workaround preemptively (i.e., entering **shut** then **no shut** on the interfaces after first switchover) prevents a failure on the subsequent switchover. CSCui49000

- After switchover, the following message may appear:

```
*Jul 23 14:20:22.196: %SYS-2-NOBLOCK: may_suspend with blocking disabled. -Process=
"RF Slave Main Thread", ipl= 0, pid= 14
```

  There is no functional impact when this message is printed.

Workaround: None. CSCui25812

- Only non-interested multicast traffic is punted to the CPU after an IOS upgrade to 151-2.SG.

  Workarounds:

  - Apply ACL on an ingress interface to deny the non-interested multicast stream, as follows:

    ```
    enderman# sh ip access-lists TAC
    Extended IP access list TAC
        10 deny ip host 10.1.1.3 host 239.1.1.5 (40 estimate matches)
        20 permit ip any any (42 estimate matches)
    ```

  - Enable PIM-SM on a dummy loopback interface by configuring ip igmp static-group x.x.x.x (where x.x.x.x is the non-interested multicast group IP address)

  CSCui64652

- A device in a guest VLAN that is connected behind a phone that is 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 more than one Equal Cost Multipath (ECMP) is available on the downstream switch, and Mediatrace is invoked to provide flow statistics, the dynamic policy does not show statistics for a flow.

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

  Workaround: None. CSCts20229

Resolved Caveats for Cisco IOS XE Release 3.3.1XO

This section lists the resolved caveats for Cisco IOS XE Release 3.3.1XO:

- If you are running "cat4500e-universalk9.SPA.03.05.00.E.152-1.E.bin c3750e-universalk9-mz.152-1.E.bin" SNMP could cause the device to suddenly crash:

  When polling the device to get an instance for CafSessionEntry object, as follows:

  ```
  Object cafSessionEntry
  OID 1.3.6.1.4.1.9.9.656.1.4.1.1
  ```

  In redundant scenarios, switchover occurs repeatedly.

  Workaround: Create SNMP view and exclude the OID, as follows:

  ```
  config t
  snmp-server view cutdown iso included
  snmp-server view cutdown 1.3.6.1.4.1.9.9.656.1.4.1.1 excluded
  snmp-server community <name> view cutdown RO
  snmp-server community <name> view cutdown RW
  ```

  CSCul24080

- If you are using dot1x and dACL and the same dACL is applied on multiple ports, one device per port, so device tracking is not substituting "ANY" with the "IP address in dACL," the dACL is either not applied on the port or deactivated on the ports on which it was previously applied.

  The following error message is observed in the output of the **debug ip admission api** command:

  ```
  002864: *Oct 17 08:39:11.698: ip_admission_api:GaliosEpm_hostPolicyUpdate: Adding 1
  ACEs to ACL NACL_xACSACLx-IP-PERMIT_ALL_TRAFFIC-5165e13c failed!
  ```

Workaround: Assign different names for the ACLs on each port. CSCuj88557

- When the same ACL is installed on two ports, ACS-configured Dynamic ACLs are neither applied nor removed from the hardware.

  Workaround: None. CSCuj99722

- While freeing routes on a device, a crash occurs if one of the following apply:
  - Configured tags (anywhere in topology) are received by a router operating with EIGRP Rel. 12 and later.
  - Query received for the route updated with tags.

  Workaround: None. CSCue78975

- On a switch running "ct5760-ipservicesk9.bin cat3k_caa-universalk9.bin cat4500e-universalk9.bin" configured with device-originated UDP services (includes but not limited to the features: TFTP, Energywise, DNS, and Cisco TrustSec, UDP based entries are not deleted from the flowmgr table resulting in a crash or poor system response, and CPU hog messages display.

  To confirm that you are affected by this bug, issue the following:

  ```
  Router# config terminal
  service internal
  end
  Router# show flowmgr
  ```

  The output lists the entries in the flowmgr table. When this issue is seen, the flowmgr entries continue to increment (i.e., flow details are still present even after the connection is closed.)

  Workaround: None.

  Reloading is required to clean up the flowmgr entries that are present in the flowmgr table. Replace tftp with ftp, if possible. CSCuh09324

- Removing the default configuration resulting from the **monitor session *id* filter packet-type good rx** command from an active SPAN session triggers HSRP and EIGRP flaps making the switch unreachable from directly connected peers.

  Workaround: Restore the default config of the **monitor session *id* filter packet-type good rx** command and issue **shut** then **no shut** on the 'err-disabled' ports. CSCui56867

- A vulnerability in the implementation of the IP version 6 (IPv6) protocol stack in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause I/O memory depletion on an affected device that has IPv6 enabled. The vulnerability is triggered when an affected device processes a malformed IPv6 packet.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-ipv6

  Note: The March 26, 2014, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2014 bundled publication.

  Individual publication links are in Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication at the following link:
  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar14.html

Workaround: See published Cisco Security Advisory CSCui59540

- A vulnerability in the Internet Key Exchange Version 2 (IKEv2) module of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a reload of the affected device that would lead to a denial of service (DoS) condition.

  The vulnerability is due to how an affected device processes certain malformed IKEv2 packets. An attacker could exploit this vulnerability by sending malformed IKEv2 packets to an affected device to be processed. An exploit could allow the attacker to cause a reload of the affected device that would lead to a DoS condition.

  Although IKEv2 is automatically enabled on a Cisco IOS Software and Cisco IOS XE Software devices when the Internet Security Association and Key Management Protocol (ISAKMP) is enabled, the vulnerability can be triggered only by sending a malformed IKEv2 packet.

  Only IKEv2 packets can trigger this vulnerability.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

  This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-ikev2

  Note: The March 26, 2014, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2014 bundled publication.

  Individual publication links are in Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication at the following link:
  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar14.html

  Workaround: See published Cisco Security Advisory CSCui88426

- A switch may leak memory in the I/O pool due to mDNS traffic. The pool in which the leak is seen is dependent on the size of the incoming packet

  Alternatively, the input queue on the interface may be stuck at the maximum size and starts to drop further traffic. This can cause pings to fail and protocols like HSRP,OSPF etc to not establish.

  This symptom occurs when mDNS traffic is sent to the switch.

  Workaround: Apply an ACL to the inbound interface. This will drop the traffic and buffers will not leak. CSCuj58950

- Multiple iterations of the **show platform cpu packet driver** command cause ARP, IGMP and other control protocols to stop processing and displays the following:

```
Switch# show platform cpu packet driver
Forerunner Packet Engine 0.28 (0)
Receive Queues: received packets summary
Qu Capac Guara CurPo Unpro Accum Kept BperP Packets
2 2512 112 2303 0 3 2511 64 339959 <--- Kept stays at 2511, Packets does not increment
8 1008 512 67 0 3 3 64 67
9 2512 304 96 0 0 0 433 96
Receive Queues: dropped packets summary
Qu Total Packets Drop No Cell Drop Overrun Drop Underrun
2 339959 100390067 0 0 <--- Drop
No Cell increments
```

  Workarounds:

  - Eliminate use of vlan 1.

  - When the switch boots, toggle "ipv6 snooping" under "vlan configuration 1" soon after switch bootup CSCuj73571

- A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

  Note: The September 23, 2009, Cisco IOS Security Advisory bundled publication includes eleven Security Advisories. Ten of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 23, 2009, or earlier.

  http://www.cisco.com/warp/public/707/cisco-sa-20090923-bundle.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_ sep09.html CSCsu70214

- When you issue either the **device-sensor accounting** or **access-session accounting attributes** command, subscriber accounting is not propagated from the switch to the ISE.

  Workaround: Don’t enable the device-sensor accounting. :CSCuj56845

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

  Workaround: Apply the following SNMP view to restrict polling of the MIB:

  ```
  snmp-server view restrict iso included
  snmp-server view restrict ciscoProcessMIB excluded
  snmp-server community mycommunity view restrict
  ```

  CSCug65204

- When authentication control direction in and mab are configured together on the interface, a MAB session is not triggered.

  Workaround: Use either the **authentication control-direction both** or **authentication open** command. CSCuo50590

- Very rarely, the following error message displays on the active supervisor engine before the standby supervisor engine achieves standby hot in SSO operating mode:

  ```
  C4K_RADIANMAN-2-SWITCHLINKBRINGUPFAILED: Stub internal link bringup failed
  ```

  This error does not impact functionality. However, the uplink ports of the standby supervisor engine loses functionality if the standby supervisor engine becomes the active supervisor engine.

  Workaround: Reinsert the standby supervisor engine. CSCui25419

Open Caveats for Cisco IOS XE Release 3.3.0XO

This section lists the open caveats for Cisco IOS XE Release 3.3.0XO:

- When an SNMP query includes the cpmCPUProcessHistoryTable, the query time is very slow, and CPU utilization of the os_info_p process (OS Info provider) increases substantially. The time required for a full walk 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 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 reboot a switch, the configured value of the interface MTU size for the elements of the port channel interface does not work for IPv6 traffic.

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

  CSCto27085

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

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

- 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

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

  Workaround: None. CSCto46018

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

  Workaround: None. CSCtu37959

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

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

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

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

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

  Workaround: None. CSCts20229

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

  The impact of stale dynamic access lists is to monitor unwanted traffic.

  Workarounds:

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

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

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

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

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

  ```
  HARDWARE WATCHDOG
  ```

  This message is not observed during a system bootup.

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

- Immediately following an SSO, the following error message may be logged by the new active route processor:

  ```
  %MRIB_PROXY-2-MRIB_RP_FAILED_LC_PORT_OPEN: RP failed in opening linecard port info for
  distributed mode, slot = 3.  MRIB updates will not be distributed to this LC.
  ```

  The error message is information only.

  Workaround: None. CSCuc72249

- On IOS Release 15.2(1)E, the DUT MAC learn rate (4700 MAC sec) is lower than the rate (8000 MAC/sec) on IOS Release 3.4.0SG. When the **macro auto monitor** command is disabled on IOS Release 15.2(1)E, the rate is 13800 MAC/sec.

  Workaround: None. CSCui07503

- When a linecard is reset on a switch using multicast, a message like the following map appear:

  ```
  PIM_REG_TUN-3-UNNUM_ERR: STANDBY
  ```

  This error is informational only.

  Workaround: None. CSCug19842

- If you configure a Qos srTCM policer with actions (traffic conform, traffic exceed, and traffic violated), the marking action for exceed traffic remains inactive.

  Workaround: Configure a policer with only conform-action and exceed-action and not with violate-action. CSCug49778.

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

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

CSCue47944

- IPv6 access-list counters do not increment when a policy-map associated with a class-map that matches a v6 ACL is applied to a physical interface and matching traffic is sent.

```
juhani07-a#sh ipv6 access-list v6acl
IPv6 access list v6acl
    permit ipv6 host 2003::2 any (1000 matches) sequence 10   --- only 1000 matched
although 2000 matching pkts sent
    permit ipv6 host 2004::2 any sequence 20
```

  Workaround: None CSCug54690

- The IOS Supplicant fails authentication when using PEAPv1 or MSChap to ACS 5.

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

- Very rarely, the following error message displays on the active supervisor engine before the standby supervisor engine achieves standby hot in SSO operating mode:

```
C4K_RADIANMAN-2-SWITCHLINKBRINGUPFAILED: Stub internal link bringup failed
```

  This error does not impact functionality. However, the uplink ports of the standby supervisor engine loses functionality if the standby supervisor engine becomes the active supervisor engine.

  Workaround: Reinsert the standby supervisor engine. CSCui25419

- On second switchover, MKA sessions go down and never recover.

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

  Applying the workaround preemptively (i.e., entering **shut** then **no shut** on the interfaces after first switchover) prevents a failure on the subsequent switchover. CSCui49000

- After switchover, the following message may appear:

```
*Jul 23 14:20:22.196: %SYS-2-NOBLOCK: may_suspend with blocking disabled. -Process=
"RF Slave Main Thread", ipl= 0, pid= 14
```

  There is no functional impact when this message is printed.

  Workaround: None. CSCui25812

Resolved Caveats for Cisco IOS XE Release 3.3.0XO

This section lists the resolved caveats for Cisco IOS XE Release 3.3.0XO:

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

  Workaround: Disable CDP on interfaces that may flap frequently. CSCub85948

- When one interface is the control-plane, EPC does not work; you cannot start packet capture.

  Workaround: None. CSCud78441

Troubleshooting

These sections provide troubleshooting guidelines for the Catalyst 4500 series switches running IOS supervisor engines:

- Netbooting from ROMMON, page 39

Netbooting from ROMMON

Netbooting using a boot loader image is not supported. Instead, use one of the following options to boot an image:

1. Boot from an SD card by entering the following command:

   ```
   rommon 1> boot slot0:<bootable_image>
   ```

2. Use ROMMON TFTP boot.

   The ROMMON TFTP boot is very similar to the BOOTLDR TFTP boot, except that:

   - the BOOTLDR variable should *not* be set
   - the TFTP server must be accessible from the Ethernet management port on the supervisor engine.

   To boot from ROMMON, perform the following tasks while in ROMMON mode:

a. Ensure that the Ethernet management port on the supervisor engine is physically connected to the network.

b. Verify that bootloader environment is not set by entering the **unset bootldr** command.

c. Set IP address of the Ethernet management port on the supervisor engine by entering the following command: **set interface fa1** *ip_address ip_mask*

   For example, to set the supervisor engine Ethernet port with an IP address 172.16.1.5 and IP mask 255.255.255.0, enter the following command:

   ```
   rommon 2> set interface fa1 172.16.1.5 255.255.255.0
   ```

d. Set default gateway for the Ethernet management port on the supervisor engine by entering the following command: **set ip route default** *gateway_ip_address*. The default gateway should be directly connected to the supervisor engine Ethernet management port subnet.

e. Ping the TFTP server to ensure that there is connectivity to the server from the Ethernet management port on the supervisor engine by entering the following command: **ping** *tftp_server_ip_address*.

f. Once the ping is successful, boot the image from the TFTP server by entering the following command: **boot tftp://***tftp_server_ip_address* **/** *image_path_and_file_name*

   For example, to boot the Cisco IOS XE image cat4500e-universalk9.03.01.00 .SG.150-1.XO.bin located on the TFTP server 172.16.1.8, enter the following command:

   ```
   rommon 3> boot tftp://172.16.1.8/tftpboot/cat4500e-universalk9.03.01.00
   .SG.150-1.XO.bin
   ```

Troubleshooting at the System Level

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.

- Ensure that you do not mix the serial and Ethernet cables plugged into the supervisor engine. The Fast Ethernet port (10/100 MGT) on the supervisor engine is inoperative. An Ethernet cable plugged into the Fast Ethernet port is active only in ROMMON mode.

Troubleshooting Modules

This section contains troubleshooting guidelines for modules:

- When you hot insert a module into a chassis, always use the ejector levers on the front of the module to seat the backplane pins properly. Inserting a module without using the ejector levers might cause the supervisor engine to display incorrect messages about the module. For module installation instructions, refer to the *Catalyst 4500 Series Module Installation Guide*.
- Whenever you connect an interface that has duplex set to autonegotiate to an end station or another networking device, ensure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the port set to autonegotiate will remain in half-duplex mode, which can cause a duplex mismatch resulting in packet loss, late collisions, and line errors on the link.

Troubleshooting MIBs

For general information on MIBs, RMON groups, and traps, refer to the Cisco public MIB directory (http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml). For information on the specific MIBs supported by the Catalyst 4500 series switches, refer to the Catalyst 4000 MIB Support List located at ftp://ftp.cisco.com/pub/mibs/supportlists/cat4000/cat4000-supportlist.html.

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:

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 3.2.X SG