Release Notes for the Catalyst 4500X Series Switches, Cisco IOS XE Release 3.3.xSG

Current release: IOS XE 3.3.2SG—November 1, 2012

Prior releases: IOS XE 3.3.1SG and 3.3.0SG

This release note describes the features, modifications, and caveats for the Cisco IOS XE 3.3.1SG software on the Catalyst 4500X Series switch,

The Cisco Catalyst 4500-X Series offers key innovations, including:

- Up-to 800 Gbps of switching capacity.
- Modular uplink and auto-detect 10 Gigabit Ethernet and 1 Gigabit Ethernet ports.
- Comprehensive virtualization capabilities, including VRF-lite and EVN.
- Redundant hot swappable fans and power supplies with AC to DC, and DC to AC failover remove single point of failure in network.
- Enhanced application monitoring through Flexible NetFlow and eight sessions of line rate bidirectional Switched Port Analyzer (SPAN)/Remote Switched Port Analyzer (RSPAN).
- Cisco TrustSec™ technology as well as robust control plane policing (CoPP) to address denial of service attacks.

Support for Cisco IOS XE Release 3.3.0SG, the default image, 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 C4500X switch, visit the following URL:

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

Contents

This publication consists of these sections:

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

Cisco IOS Software Packaging

The Enterprise Services image supports all Cisco Catalyst 4500 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.

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

Topics include:

Feature Support by Image Type

Table 1 is a detailed list of features supported on Catalyst 4500X Series switches running Cisco IOS Software Release 3.3.1SG categorized by image type. Please visit Feature Navigator for package details:

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

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
2-way Community Private VLANs	Yes	Yes
8-Way CEF Load Balancing	Yes	Yes
10 Gigabit Uplink Use	Yes	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
AAA Server Group	Yes	Yes
AAA Server Group Based on DNIS	Yes	Yes
ACL - Improved Merging Algorithm	Yes	Yes
ACL Logging	Yes	Yes
ACL Policy Enhancements	Yes	Yes
ACL Sequence Numbering	Yes	Yes
Address Resolution Protocol (ARP)	Yes	Yes
ANCP Client	Yes	Yes
ANSI TIA-1057 LLDP - MED Location Extension	Yes	Yes
ANSI TIA-1057 LLDP - MED Support	Yes	Yes
ARP Optimization	Yes	Yes
Auto QoS	Yes	Yes
Auto SmartPorts	Yes	Yes
Auto-MDIX	Yes	Yes
Auto-Voice VLAN (part of Auto QoS)	Yes	Yes
AutoInstall Using DHCP for LAN Interfaces	Yes	Yes
AutoQoS - VoIP	Yes	Yes
AutoRP Enhancement	Yes	Yes
BGP	No	Yes
BGP 4	No	Yes
BGP 4 4Byte ASN (CnH)	No	Yes
BGP 4 Multipath Support	No	Yes
BGP 4 Prefix Filter and In-bound Route Maps	No	Yes
BGP 4 Soft Config	No	Yes
BGP Conditional Route Injection	No	Yes
BGP Configuration Using Peer Templates	No	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

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

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
Class Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)	Yes	Yes
Class-Based Marking	Yes	Yes
Class-Based Policing	Yes	Yes
Class-Based Shaping	Yes	Yes
Clear Counters Per Port	Yes	Yes
CLI String Search	Yes	Yes
CNS	Yes	Yes
CNS - Configuration Agent	Yes	Yes
CNS - Event Agent	Yes	Yes
CNS - Image Agent	Yes	Yes
CNS - Interactive CLI	Yes	Yes
CNS Config Retrieve Enhancement with Retry and Interval	Yes	Yes
Command Scheduler (Kron)	Yes	Yes
Command Scheduler (Kron) Policy for System Startup	Yes	Yes
Commented IP Access List Entries	Yes	Yes
Community Private VLAN	Yes	Yes
Configuration Change Tracking Identifier	Yes	Yes
Configuration Change Notification and Logging	Yes	Yes
Configuration Replace and Configuration Rollback	Yes	Yes
Configuration Rollback Confirmed Change	Yes	Yes
Contextual Configuration Diff Utility	Yes	Yes
Control Plane Policing (Copp)	Yes	Yes
CPU Enhancement	Yes	Yes
CPU Optimization for Layer 3 Multicast Control Packets	Yes	Yes
Critical Authorization for Voice and Data	Yes	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

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

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
ErrDisable timeout	Yes	Yes
EtherChannel	Yes	Yes
EtherChannel Flexible PAgP	Yes	Yes
EtherChannel Enhancement - Single Port Channel	Yes	Yes
Fast EtherChannel (FEC)	Yes	Yes
FHRP - Enhanced Object Tracking of IP SLAs[1]	Yes	Yes
FHRP - EOT integration with EEM	Yes	Yes
FHRP - GLBP - IP Redundancy API	Yes	Yes
FHRP - HSRP - Hot Standby Router Protocol V2	Yes	Yes
FHRP - Object Tracking List	Yes	Yes
Filter-ID Based ACL Application	Yes	Yes
FIPS 140-2/3 Level 2 Certification	Yes	Yes
Flexible NetFlow - Full Flow support	Yes	Yes
Flexible NetFlow - Ingress support	Yes	Yes
Flexible NetFlow - IPv4 Unicast Flows	Yes	Yes
Flexible NetFlow - IPv6 Unicast Flows	Yes	Yes
Flexible NetFlow - Layer 2 Fields	Yes	Yes
Flexible NetFlow - Multiple User Defined Caches	Yes	Yes
Flexible NetFlow - NetFlow Export over IPv4	Yes	Yes
Flexible NetFlow - NetFlowV5 Export protocol	Yes	Yes
Flexible NetFlow - NetFlow v9 Export Format	Yes	Yes
Flexible NetFlow - VLAN ID support	Yes	Yes
Flex Links+(VLAN Load balancing)	Yes	Yes
Embedded Event Manager (EEM) 3.2	Yes	Yes
Forced 10/100 Autonegotiation	Yes	Yes
FTP Support for Downloading Software Images	Yes	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

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

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

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

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

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

Table 1 *IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E*

Feature	IP Base	Enterprise Services
IP SLAs - Sub-millisecond Accuracy Improvements	Yes	Yes
IP SLAs - TCP Connect Operation	Yes	Yes
IP SLAs - UDP Based VoIP Operation	Yes	Yes
IP SLAs - UDP Echo Operation	Yes	Yes
IP SLAs - UDP Jitter Operation	Yes	Yes
IP SLAs - VoIP Threshold Traps	Yes	Yes
IP Summary Address for RIPv2	Yes	Yes
IP Unnumbered for VLAN-SVI interfaces	Yes	Yes
IPSG (IP Source Guard) v4	Yes	Yes
IPSG (IP Source Guard) v4 for Static Hosts	Yes	Yes
IPv4 Routing: Static Hosts/Default Gateway	Yes	Yes
IPv6 - BGP	No	Yes
IPv6 - CNS Agents	Yes	Yes
IPv6 - Config Logger	Yes	Yes
IPv6 HSRP	Yes	Yes
IPv6 - HTTP(S)	Yes	Yes
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	Yes	Yes
IPv6 - TCL	Yes	Yes
IPv6 (Internet Protocol Version 6)	Yes	Yes
IPv6 Access Services: DHCPv6 Relay Agent	Yes	Yes
IPv6 Interface Statistics	Yes	Yes
IPv6 MLD Snooping v1 and v2	Yes	Yes
IPv6 MTU Path Discovery	Yes	Yes
IPv6 Multicast	Yes	Yes
IPv6 Multicast: Bootstrap Router (BSR)	No	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
IPv6 Multicast: Explicit Tracking of Receivers	Yes	Yes
IPv6 Multicast: MLD Access Group	Yes	Yes
IPv6 Multicast: Multicast Listener Discovery (MLD) Protocol, Versions 1 and 2	Yes	Yes
IPv6 Multicast: PIM Accept Register	Yes	Yes
IPv6 Multicast: PIM Embedded RP Support	Yes	Yes
IPv6 Multicast: PIM Source-Specific Multicast (PIM-SSM)	Yes	Yes
IPv6 Multicast: PIM Sparse Mode (PIM-SM)	Yes	Yes
IPv6 Multicast: Routable Address Hello Option	Yes	Yes
IPv6 Multicast: RPF Flooding of Bootstrap Router (BSR) Packets	Yes	Yes
IPv6 Multicast: Scope Boundaries	Yes	Yes
IPv6 Neighbor Discovery	Yes	Yes
Identity 4.1 Network Edge Access Topology	Yes	Yes
IPv6 RA Guard	Yes	Yes
IPV6 Router Advertisement (RA) Guard	Yes	Yes
IPv6 Routing - EIGRP Support	Yes	Yes
IPv6 Routing: OSPF for IPv6 (OSPFv3)	Yes[3]	Yes
IPv6 Routing: RIP for IPv6 (RIPng)	Yes	Yes
IPv6 Routing: Route Redistribution	Yes	Yes
IPv6 Routing: Static Routing	Yes	Yes
IPv6 Security: Secure Shell SSH support over IPv6	Yes	Yes
IPv6 Services: AAAA DNS Lookups over an IPv4 Transport	Yes	Yes
IPv6 Services: Cisco Discovery Protocol (CDP) - IPv6 Address Family Support for Neighbor Information	Yes	Yes
IPv6 Services: DNS Lookups over an IPv6 Transport	Yes	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
IPv6 Services: Extended Access Control Lists	Yes	Yes
IPv6 Services: Standard Access Control Lists	Yes	Yes
IPv6 Stateless Auto-configuration	Yes	Yes
IPv6 Switching: CEF Support	Yes	Yes
IPv6 Switching: CEFv6 Switched Automatic IPv4-compatible Tunnels (in software)	Yes	Yes
IPv6 Switching: CEFv6 Switched Configured IPv6 over IPv4 Tunnels (in software)	Yes	Yes
IPv6 Switching: CEFv6 Switched ISATAP Tunnels (in software)	Yes	Yes
IPv6 Tunneling: Automatic 6to4 Tunnels (in software)	Yes	Yes
IPv6 Tunneling: Automatic IPv4-compatible Tunnels (in software)	Yes	Yes
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels (in software)	Yes	Yes
IPv6 Tunneling: ISATAP Tunnel Support (in software)	Yes	Yes
IPv6 Tunneling: Manually Configured IPv6 over IPv4 Tunnels (in software)	Yes	Yes
IPv6 Anycast Address	Yes	Yes
IPv6 ICMPv6	Yes	Yes
IPv6 ICMPv6 Redirect	Yes[3]	Yes
IPv6 OSPFv3 NSF/SSO	Yes[3]	Yes
IPv6 OSPFv3 Fast Convergence	Yes	Yes
IPv6 Neighbor Discovery Duplicate Address Detection	Yes	Yes
IPsecv3/IKEv2 (for management traffic only)	Yes	Yes
IS-IS for IPv4 and IPv6	No	Yes
ISSU (IOS In-Service Software Upgrade)	Yes	Yes
Jumbo Frames	Yes	Yes
Layer 2 Control Packet	Yes	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
Layer 2 Protocol Tunneling (L2PT)	Yes	Yes
Layer 2 Traceroute	Yes	Yes
Layer 3 Multicast Routing (PIM SM, SSM, Bidir)	Yes	Yes
Link State Tracking	Yes	Yes
Loadsharing IP packets over more than six parallel paths	Yes	Yes
Local Proxy ARP	Yes	Yes
Location MIBs	Yes	Yes
MAB for Voice VLAN	Yes	Yes
MAB with Configurable User Name/Password	Yes	Yes
MAC Address Notification	Yes	Yes
MAC Authentication Bypass	Yes	Yes
MAC Move and Replace	Yes	Yes
Management IPV6 port	Yes	Yes
Medianet 2.0: AutoQoS SRND4 Macro	Yes	Yes
Medianet 2.0: Integrated Video Traffic Simulator (hardware-assisted IP SLA); IPSLA generator and responder	Yes	Yes
Medianet 2.0: Flow Metadata	Yes	Yes
Medianet 2.0: Media Service Proxy	Yes	Yes
Medianet 2.0: Media Monitoring (Performance Monitoring and Mediatrace)	Yes	Yes
Memory Threshold Notifications	Yes	Yes
Microflow policers	Yes	Yes
Modular QoS CLI (MQC)	Yes	Yes
Multi-authentication and VLAN Assignment	Yes	Yes
Multi-VRF Support (VRF lite)	No	Yes
Multicast BGP (MBGP)	No	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
Multicast Fast Switching Performance Improvement	Yes	Yes
Multicast Routing Monitor (MRM)	Yes	Yes
Multicast Source Discovery Protocol (MSDP)	Yes	Yes
Multicast Subsecond Convergence	Yes	Yes
NAC - L2 IEEE 802.1x	Yes	Yes
NAC - L2 IP	Yes	Yes
ND Cache Limit/Interface	Yes	Yes
NETCONF over SSHv2	Yes	Yes
Network Edge Access Topology (NEAT)	Yes	Yes
NEAT Enhancement: Re-Enabling BPDU Guard Based on User Configuration	Yes	Yes
Network Time Protocol (NTP)	Yes	Yes
Network Time Protocol (NTP) master	Yes	Yes
NMSP Enhancements • GPS support for location • Location at switch level • Local timezone change • Name value pair • Priority settings for MIBs	Yes	Yes
No Service Password Recovery	Yes	Yes
No. of VLAN Support	4096	4096
NSF - BGP	No	Yes
NSF - EIGRP	Yes	Yes
NSF - OSPF (version 2 only)	Yes	Yes
NTP for IPv6	Yes	Yes
NTP for VRF aware	No	Yes
Onboard Failure Logging (OBFL)	Yes	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
OSPF	Yes[3]	Yes
OSPF v3 Authentication	Yes[3]	Yes
OSPF Flooding Reduction	Yes[3]	Yes
OSPF for Routed Access	Yes	Yes
OSPF Incremental Shortest Path First (i-SPF) Support	Yes[3]	Yes
OSPF Link State Database Overload Protection	Yes[3]	Yes
OSPF Not-So-Stubby Areas (NSSA)	Yes[3]	Yes
OSPF Packet Pacing	Yes[3]	Yes
OSPF Shortest Paths First Throttling	Yes[3]	Yes
OSPF Stub Router Advertisement	Yes[3]	Yes
OSPF Support for Fast Hellos	Yes[3]	Yes
OSPF Support for Link State Advertisement (LSA) Throttling	Yes[3]	Yes
OSPF Support for Multi-VRF on CE Routers	Yes[3]	Yes
OSPF Update Packet-Pacing Configurable Timers	Yes[3]	Yes
Per Intf IGMP State Limit	Yes	Yes
Per Intf MrouteState Limit	Yes	Yes
Per Port Per VLAN Policing	Yes	Yes
Per-User ACL Support for 802.1X/MAB/Webauth users	Yes	Yes
Per-VLAN Learning	Yes	Yes
PIM Dense Mode State Refresh	Yes	Yes
PIM Multicast Scalability	Yes	Yes
PIM Version 1	Yes	Yes
PIM Version 2	Yes	Yes
PoEP via LLDP	Yes	Yes
Policy Based Routing (PBR)	No	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
Port Security	Yes	Yes
Port Security on Etherchannel Trunk Port	Yes	Yes
Pragmatic General Multicast (PGM)	Yes	Yes
Priority Queueing (PQ)	Yes	Yes
Private VLAN Promiscuous Trunk Port	Yes	Yes
Private VLAN Trunk Ports	Yes	Yes
Private VLANs	Yes	Yes
Propagation of Location Info over CDP	Yes	Yes
PVLAN over EtherChannel	Yes	Yes
PVST + (Per VLAN Spanning Tree Plus)	Yes	Yes
Q-in-Q	Yes	Yes
QoS Packet Marking	Yes	Yes
QoS Priority Percentage CLI Support	Yes	Yes
RADIUS	Yes	Yes
RADIUS Attribute 44 (Accounting Session ID) in Access Requests	Yes	Yes
RADIUS Change of Authorization	Yes	Yes
Rapid PVST+ Dispute Mechanism	Yes	Yes
Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)	Yes	Yes
Reduced MAC Address Usage	Yes	Yes
Redundancy Facility Protocol	Yes	Yes
Remote SPAN (RSPAN)	Yes	Yes
REP (Resilient Ethernet Protocol)	Yes	Yes
REP - No Edge Neighbour Enhancement	Yes	Yes
RIP v1	Yes	Yes
RMON events and alarms	Yes	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
Secure Copy (SCP)	Yes	Yes
Secure Shell SSH Version 1 Integrated Client	Yes	Yes
Secure Shell SSH Version 1 Server Support	Yes	Yes
Secure Shell SSH Version 2 Client Support	Yes	Yes
Secure Shell SSH Version 2 Server Support	Yes	Yes
Single Rate 3-Color Marker for Traffic Policing	Yes	Yes
Smart Port	Yes	Yes
SNMP (Simple Network Management Protocol)	Yes	Yes
SNMP Inform Request	Yes	Yes
SNMP Manager	Yes	Yes
SNMPv2C	Yes	Yes
SNMPv3 - 3DES and AES Encryption Support	Yes	Yes
SNMPv3 (SNMP Version 3)	Yes	Yes
Source Specific Multicast (SSM)	Yes	Yes
Source Specific Multicast (SSM) - IGMPv3,IGMP v3lite, and URD	Yes	Yes
Source Specific Multicast (SSM) Mapping	Yes	Yes
Span Enhancement: Packet Type and Address Type Filtering	Yes	Yes
Spanning Tree Protocol (STP)	Yes	Yes
Spanning Tree Protocol (STP) - Backbone Fast Convergence	Yes	Yes
Spanning Tree Protocol (STP) - Loop Guard	Yes	Yes
Spanning Tree Protocol (STP) - Portfast	Yes	Yes
Spanning Tree Protocol (STP) - PortFast BPDU Filtering	Yes	Yes
Spanning Tree Protocol (STP) - Portfast BPDU Guard	Yes	Yes
Spanning Tree Protocol (STP) - Portfast Support for Trunks	Yes	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
Spanning Tree Protocol (STP) - Root Guard	Yes	Yes
Spanning Tree Protocol (STP) - Uplink Fast Convergence	Yes	Yes
Spanning Tree Protocol (STP) - Uplink Load Balancing	Yes	Yes
Spanning Tree Protocol (STP) Extension	Yes	Yes
SSO - HSRP	Yes	Yes
SSO - IGMP Snooping	Yes	Yes
Standard IP Access List Logging	Yes	Yes
Standby Supervisor Port Usage	Yes	Yes
Sticky Port Security	Yes	Yes
Sticky Port Security on Voice VLAN	Yes	Yes
Storm Control - Per-Port Multicast Suppression	Yes	Yes
STP Syslog Messages	Yes	Yes
Stub IP Multicast Routing	Yes	Yes
Sub-second UDLD	Yes	Yes
SVI (Switch Virtual Interface) Autostate Exclude	Yes	Yes
Switch and IP Phone Security Interaction	Yes	Yes
Switch Port Analyzer (SPAN)	Yes	Yes
Switch Port Analyzer (SPAN) - CPU Source	Yes	Yes
Syslog over IPV6	Yes	Yes
System Logging - EAL4 Certification Enhancements	Yes	Yes
TACACS SENDAUTH function	Yes	Yes
TACACS Single Connection	Yes	Yes
TACACS+	Yes	Yes
TACACS+ and Radius for IPv6-	Yes	Yes
TCAM4 - Dynamic Multi-Protocol	Yes	Yes
TCAM4 - Service-Aware Resource Allocation	Yes	Yes

Table 1 IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500X Series Supervisor Engine 7-E

Feature	IP Base	Enterprise Services
Time Domain Reflectometry (TDR)	Yes	Yes
Time-Based Access Lists	Yes	Yes
Time-Based Access Lists Using Time Ranges (ACL)	Yes	Yes
Trusted boundary (extended trust for CDP devices)	Yes	Yes
TrustSec SGT Exchange Protocol (SXP) IPv4	Yes	Yes
UDI - Unique Device Identifier	Yes	Yes
Uni-Directional Link Routing (UDLR)	Yes	Yes
Unicast Mac Filtering	Yes	Yes
Unicast Reverse Path Forwarding (uRPF)	Yes	Yes
Unidirectional Ethernet	Yes	Yes
UniDirectional Link Detection (UDLD)	Yes	Yes
Virtual Router Redundancy Protocol (VRRP)	Yes	Yes
Virtual Trunking Protocol (VTP) - Pruning	Yes	Yes
VLAN Access Control List (VACL)	Yes	Yes
VLAN MAC Address Filtering	Yes	Yes
VLAN Mapping (VLAN Translation)	Yes	Yes
VRF-aware TACACS+	No	Yes
VTP (Virtual Trunking Protocol) Version 2	Yes	Yes
VTP Version 3	Yes	Yes
WCCP Version 2	Yes	Yes
Web Authentication Proxy	Yes	Yes
Webauth Enhancements	Yes	Yes
Wireshark-based Ethernet Analyzer	Yes	Yes
XML-PI	Yes	Yes

[1] FHRP - Enhanced Object Tracking of IP SLAs is not supported in LANBase.

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

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

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 4500X Series Switches

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

- CISCO-IETF-IP-FORWARD-MIB
- CISCO-IETF-IP-MIB
- LLDP HA
- SSO
- WCCP Version 1
- TrustSec: IEEE 802.1ae MACSec Layer 2 encryption
- TrustSec: IEEE 802.1ae MACSec encryption on user facing ports
- TrustSec: IEEE 802.1ae MACSec encryption on user facing ports SSO
- TrustSec: IEEE 802.1ae MACSec encryption between switch-to-switch links using Cisco SAP (Security Association Protocol)

Orderable Product Numbers

Table 2 Cisco IOS Software Release 3.3.1SG Product Numbers and Images for the Catalyst 4500X Series Switches

Product Number	Description	Image
Base Switch PIDs		
WS-C4500X-32SFP+	Catalyst 4500-X 32 Port 10GE IP Base, Front-to-Back Cooling i.e. Port Side to Power Supply Cooli	cat4500e-universal.SPA.03.03.00.SG.151-1.SG.bin cat4500e-universalk9.SPA.03.03.00.SG.151-1.SG.bin
WS-C4500X-F-32SFP+	Catalyst 4500-X 32 Port 10GE IP Base, Back-to-Front Cooling i.e. Power Supply to Port Side Cooling	cat4500e-universal.SPA.03.03.00.SG.151-1.SG.bin cat4500e-universalk9.SPA.03.03.00.SG.151-1.SG.bin
WS-C4500X-16SFP+	Catalyst 4500-X 16 Port 10GE IP Base, Front-to-Back Cooling i.e. Port Side to Power Supply Cooling with 1PS	cat4500e-universal.SPA.03.03.01.SG.151-1.SG1.bin cat4500e-universal.SPA.03.03.01.SG.151-1.SG1.bin

Table 2 Cisco IOS Software Release 3.3.1SG Product Numbers and Images for the Catalyst 4500X Series Switches

Product Number	Description	Image
WS-C4500X-F-16SFP+	Catalyst 4500-X 16 Port 10GE IP Base, Back-to-Front Cooling i.e. Power Supply to Port Side Cooling with 1PS	cat4500e-universal.SPA.03.03.01.SG.151-1.SG1.bin cat4500e-universal.SPA.03.03.01.SG.151-1.SG1.bin
WS-C4500X-24X-ES	Catalyst 4500-X 24 Port 10GE IP Base, Front-to-Back Cooling i.e. Port Side to Power Supply Cooling with 2PS	cat4500e-universal.SPA.03.03.01.SG.151-1.SG1.bin cat4500e-universal.SPA.03.03.01.SG.151-1.SG1.bin
FRU and OIR FANs		
C4KX-FAN-F	Catalyst 4500-X Back-to-Front Cooling Fan	NA
C4KX-FAN-R	Catalyst 4500-X Front-to-Back Cooling Fan	NA
Power Supply		
C4KX-PWR-750AC-F	Catalyst 4500-X 750W AC Back-to-Front Cooling Power Supply	NA
C4KX-PWR-750AC-R	Catalyst 4500-X 750W AC Front-to-Back Cooling Power Supply	NA
C4KX-PWR-750DC-F	Catalyst 4500-X 750W DC Back-to-Front Cooling Power Supply	NA
C4KX-PWR-750DC-R	Catalyst 4500-X 750W DC Front-to-Back Cooling Power Supply	NA
Accessories		
CAB-CON-C4K-RJ45	Console Cable 6ft with RJ-45-to-RJ-45	NA
SD-X45-2GB-E	Cisco Catalyst 4500 2-GB SD card	NA
USB-X45-4GB-E	Cisco Catalyst 4500 4-GB USB device	NA
Software		
S45XU-33-1511SG	Cisco Catalyst 4500-X Cisco IOS Software XE Release 3.3.0 SG/3.3.1 SG noncrypto universal image	cat4500e-universal.SPA.03.03.00.SG.151-1.SG.bin cat4500e-universal.SPA.03.03.01.SG.151-1.SG1.bin

Table 2 Cisco IOS Software Release 3.3.1SG Product Numbers and Images for the Catalyst 4500X Series Switches

Product Number	Description	Image
S45XUK9-33-1511SG	Cisco Catalyst 4500-X Cisco IOS Software XE Release 3.3.0 SG/3.3.1 SG crypto universal	cat4500e-universalk9.SPA.03.03.00.SG.151-1.SG.bin cat4500e-universalk9.SPA.03.03.01.SG.151-1.SG1.bin
C4500X-LIC=	Base product ID for software upgrade licenses on Catalyst 4500-X (paper delivery)	NA
C4500X-IPB	Catalyst 4500-X IP BASE software license (paper delivery)	NA
C4500X-IP-ES	Catalyst 4500-X IP BASE to Enterprise Services upgrade license (paper delivery)	NA
L-C4500X-LIC=	Catalyst 4500-X Base product ID for software upgrade licenses (electronic delivery)	NA
L-C4500X-IPB	Catalyst 4500-X IP BASE software license (electronic delivery)	NA
L-C4500X-IP-ES	Catalyst 4500-X IP BASE to Enterprise Services upgrade license (electronic delivery)	NA

Support

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

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

Supported Hardware on the Catalyst 4500X Series Switches

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

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

Table 3 lists the hardware supported on the Catalyst 4500X Series switches.

Table 3 Supported Hardware on the Cisco Catalyst 4500X Series Switch

Product Number (append with "=" for spares)	**Product Description**
Small Form-Factor Pluggable Gigabit Ethernet Modules	
GLC-BX-D	1000BASE-BX10-D small form-factor pluggable module For DOM support, see Table 6 on page 26.
GLC-BX-U	1000BASE-BX10-U small form-factor pluggable module For DOM support, see Table 6 on page 26.bv
GLC-SX-MM	1000BASE-SX small form-factor pluggable module
GLC-SX-MMD	1000BASE-SX small form-factor pluggable module
GLC-LH-SM	1000BASE-LX/LH small form-factor pluggable module
GLC-LH-SMD	1000BASE-LX/LH small form-factor pluggable module with DOM support
GLC-ZX-SM	1000BASE-ZX small form-factor pluggable module
GLC-T	1000BASE-T small form-factor pluggable module
CWDM-SFP-xxxx	CWDM small form-factor pluggable module (See Table 4 on page 24 for a list of supported wavelengths.) For DOM support, see Table 6 on page 26.
SFP+ Modules	
SFP-10G-SR	Cisco 10GBASE-SR SFP+ Module for MMF
SFP-10G-LR	Cisco 10GBASE-LR SFP+ Module for SMF
SFP-10G-LRM	Cisco 10GBASE-LRM SFP+ Module for MMF
SFP-H10GB-CU1M	10GBASE-CU SFP+ Cable 1 Meter
SFP-H10GB-CU3M	10GBASE-CU SFP+ Cable 3 Meter
SFP-H10GB-CU5M	10GBASE-CU SFP+ Cable 5 Meter
SFP-10G-ER	Cisco 10GBASE-ER SFP+ Module for SMF
SFP-10G-ZR	Cisco 10GBASE-ZR SFP+ Module for SMF **Note** This module is only supported on the uplink module in the back-to-front airflow configuration.

Table 4 briefly describes the supported CWDM wavelengths in the Catalyst 4500X Series switch.

Table 4 CWDM SFP Supported Wavelengths on the Cisco Catalyst 4500X Series Switches

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

Table 4 CWDM SFP Supported Wavelengths on the Cisco Catalyst 4500X Series Switches

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

Table 5 briefly describes the supported DWDM wavelengths on the Catalyst 4500X Series Switches.

Table 5 DWDM SFP Supported Wavelengths on the Cisco Catalyst 4500X Series Switches

Product Number (append with "=" for spares)	**Product Description**
DWDM-SFP-6141=	Cisco 1000BASE-DWDM SFP 1561.42 nm
DWDM-SFP-6061=	Cisco 1000BASE-DWDM SFP 1560.61 nm
DWDM-SFP-5979=	Cisco 1000BASE-DWDM SFP 1559.79 nm
DWDM-SFP-5898=	Cisco 1000BASE-DWDM SFP 1558.98 nm
DWDM-SFP-5817=	Cisco 1000BASE-DWDM SFP 1558.17 nm
DWDM-SFP-5736=	Cisco 1000BASE-DWDM SFP 1557.36 nm
DWDM-SFP-5655=	Cisco 1000BASE-DWDM SFP 1556.55 nm
DWDM-SFP-5575=	Cisco 1000BASE-DWDM SFP 1555.75 nm
DWDM-SFP-5494=	Cisco 1000BASE-DWDM SFP 1554.94 nm
DWDM-SFP-5413=	Cisco 1000BASE-DWDM SFP 1554.13 nm
DWDM-SFP-5332=	Cisco 1000BASE-DWDM SFP 1553.33 nm
DWDM-SFP-5252=	Cisco 1000BASE-DWDM SFP 1552.52 nm
DWDM-SFP-5172=	Cisco 1000BASE-DWDM SFP 1551.72 nm
DWDM-SFP-5092=	Cisco 1000BASE-DWDM SFP 1550.92 nm
DWDM-SFP-5012=	Cisco 1000BASE-DWDM SFP 1550.12 nm
DWDM-SFP-4931=	Cisco 1000BASE-DWDM SFP 1549.32 nm
DWDM-SFP-4851=	Cisco 1000BASE-DWDM SFP 1548.51 nm
DWDM-SFP-4772=	Cisco 1000BASE-DWDM SFP 1547.72 nm
DWDM-SFP-4694=	Cisco 1000BASE-DWDM SFP 1542.94 nm
DWDM-SFP-4692=	Cisco 1000BASE-DWDM SFP 1546.92 nm
DWDM-SFP-4614=	Cisco 1000BASE-DWDM SFP 1542.14 nm
DWDM-SFP-4612=	Cisco 1000BASE-DWDM SFP 1546.12 nm
DWDM-SFP-4532=	Cisco 1000BASE-DWDM SFP 1545.32 nm
DWDM-SFP-4453=	Cisco 1000BASE-DWDM SFP 1544.53 nm
DWDM-SFP-4373=	Cisco 1000BASE-DWDM SFP 1543.73 nm

Table 5 DWDM SFP Supported Wavelengths on the Cisco Catalyst 4500X Series Switches

Product Number (append with "=" for spares)	**Product Description**
DWDM-SFP-4134=	Cisco 1000BASE-DWDM SFP 1541.35 nm
DWDM-SFP-4056=	Cisco 1000BASE-DWDM SFP 1540.56 nm
DWDM-SFP-3977=	Cisco 1000BASE-DWDM SFP 1539.77 nm
DWDM-SFP-3898=	Cisco 1000BASE-DWDM SFP 1539.98 nm
DWDM-SFP-3819=	Cisco 1000BASE-DWDM SFP 1538.19 nm
DWDM-SFP-3739=	Cisco 1000BASE-DWDM SFP 1537.40 nm
DWDM-SFP-3661=	Cisco 1000BASE-DWDM SFP 1536.61 nm
DWDM-SFP-3582=	Cisco 1000BASE-DWDM SFP 1535.82 nm
DWDM-SFP-3504=	Cisco 1000BASE-DWDM SFP 1535.04 nm
DWDM-SFP-3425=	Cisco 1000BASE-DWDM SFP 1534.25 nm
DWDM-SFP-3346=	Cisco 1000BASE-DWDM SFP 1533.47 nm
DWDM-SFP-3268=	Cisco 1000BASE-DWDM SFP 1532.68 nm
DWDM-SFP-3190=	Cisco 1000BASE-DWDM SFP 1531.90 nm
DWDM-SFP-3112=	Cisco 1000BASE-DWDM SFP 1531.12 nm
DWDM-SFP-3033=	Cisco 1000BASE-DWDM SFP 1530.33 nm

For a complete list of Cisco Gigabit Ethernet Transceiver Modules, please refer to the URL:

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

Table 6 briefly describes the DOM support on the Catalyst 4500X Series switches.

Table 6 DOM Support on the Cisco Catalyst 4500X Series Switches

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

New and Changed Information

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

- New Software Features in Release IOS XE 3.3.1SG, page 27
- New Hardware Features in Release IOS XE 3.3.1SG, page 27
- New Software Features in Release IOS XE 3.3.0SG, page 27

New Software Features in Release IOS XE 3.3.1SG

Release IOS XE 3.3.1SG provides no new new software on the Catalyst 4500X Series switch.

New Hardware Features in Release IOS XE 3.3.1SG

Release IOS XE 3.3.1SG provides the following new hardware on the Catalyst 4500X Series switch:

- Catalyst 4500-X 16 Port 10GE IP Base
- 9000W

New Software Features in Release IOS XE 3.3.0SG

Release IOS XE 3.3.0SG provides the following new software on the Catalyst 4500X-32 Switch in addition to the features present in the previous XE release on the Catalyst 4500E:

- IOS Based Device profiling
- SXP Syslog enhancement
- Medianet 2.0
  - Media Monitoring (includes Performance Monitoring and Mediatrace)
  - Flow MetaData
  - Media Services Proxy
  - Integrated video traffic simulator (hardware assisted IP SLA)

    IPSLA generator and responder
  - AutoQoS Macro
- Medianet2.0:NMSP enhancements
  - Location at switch level
  - Local timezone change
  - GPS support for location
  - Priority settings for MIBs
  - Name value pair
- EnergyWise Version 2.5

  For details refer to the URLs:

http://www.cisco.com/en/US/products/ps10195/index.html

http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2_5/ios/release/notes/ol23554.html

- Wireshark- based Ethernet Analyzer
- IPv6 OSPFv3 NSF/SSO
- IPv6 OSPFv3 Fast Convergence
- OSPFv3 Authentication
- IPsecv3/IKEv2 (for management traffic only)
- FIPS 140-2/3 Level 2 Certification
- No Service Password Recovery
- Easy Virtual Network (EVN)
- ND cache limit per interface
- HSRPv2 for IPv6 Global Address Support
- MAB with configurable user name/ password
- BGP Wildcard
- 802.1X with User Distribution ("Configuring 802.1X Port-Based Authentication" chapter)
- Auto SmartPort ("Configuring Auto SmartPort Macros" chapter)
- DSCP/CoS via LLDP ("Configuring LLDP, LLDP-MED, and Location Service" chapter
- EEM: Embedded Event Manager 3.2

  For details, refer to the URL:

  http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/system_management/configuration/guide/sm_12eem.html
- EIGRP Service Advertisement Framework

  For details refer to the URL:

  http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/saf_cg.html
- EnergyWise 2.5

  For details refer to the URLs:

  http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2/ios/configuration/guide/ew_v2.html

  http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2_5/ios/release/notes/ol23554.html#wp604941
- GOLD Online Diagnostics ("Performing Diagnostics" chapter)
- ACL Policy Enhancements ("Configuring Network Security with ACLs" chapter)
- Network Edge Access Topology ("Configuring 802.1X Port-Based Authentication" chapter)
- IPSG for Static Hosts (Refer to the Cisco IOS library)
- IPv6 PACL ("Configuring Network Security with ACLs" chapter)

- IPv6 RA Guard ("Configuring Network Security with ACLs" chapter)
- IPv6 Interface Statistics ("Configuring Layer 3 Interfaces" chapter)
- IS-IS for IPv4 ad IPv6 (Refer to the Cisco IOS library)
- IEEE 802.3ad Link Aggregation (LACP) Port-Channel Standalone Disable
- Layer 2 Control Packet)
- Link State Tracking ("Configuring EtherChannel and Link State Tracking" chapter)
- MAC move and replace ("Administering the Switch" chapter)
- Per-VLAN Learning ("Administering the Switch" chapter)
- PoEP via LLDP ("Configuring LLDP, LLDP-MED, and Location Service" chapter)
- RADIUS CoA ("Configuring 802.1X Port-Based Authentication" chapter)
- Sub-second UDLD (Configuring UDLD" chapter)
- VLAN Translation ("Configuring 802.1Q Tunneling, VLAN Mapping, and Layer 2 Protocol Tunneling" chapter)
- VRF-aware TACACS+ ("Configuring VRF-lite" chapter)
- XML Programmatic Interface (Refer to the Cisco IOS library)

  For details refer to the URL:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_xmlpi_v1.html
- BGP 4Byte ASN (CnH)
- BGP graceful restart per neighbor
- BGP Nexthop tracking
- Dynamic PBR API
- Multicast Call Admission Control—Per interface route state limit
- Bandwidth-based Call Admission Control policy for Multicast
- Ability to disallow mcast group ranges
- IPv6 SSM mapping—MLD v1 receivers
- IPv6 BSR—Ability to configure RP mapping
- MSDP MD5 password authentication
- MLD group limits
- IPv6 multicast—Disable group ranges
- IGMP static group range support
- PIM-triggered joins
- Support directly conn. add in autoRP cand. RP
- Enhanced Multicast Multipath
- IGMP-STD-MIB implementation
- Knob to use SNMP MIBII ifindex as int-id in OSPF data fields
- Enhanced OSPF traffic stats
- OSPF Mechanism to exclude Connected prefixes

- OSPF TTL Security Check
- OSPF Graceful Shutdown
- OSPFv2 int. enabling—OSPF area command
- OSPFv3 IPSec enhancements
- IP-RIP: Delayed startup
- AAA accounting: Stop record CLI enhancement
- Radius Server Load Balancing porting
- AAA Double Authentication Secured by Absolute Timeout
- Local AAA Attribute Support via Subscriber Profile
- Method List, Server Group Scalability
- BGP: Dual AS Accept Implementation
- NSF in IP Base
- IGMPv3 Host Stac
- Per Intf IGMP State Limit
- Per Intf MrouteState Limit
- TACACS+ and Radius for IPv6
- NTP for IPv6(It is VRF aware as well)

Cisco IOS XE to Cisco IOS Version Number Mapping

As Table 7 shows, each version of Cisco IOS XE has an associated Cisco IOS version:

Table 7 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOS Version
03.1.0SG	15.0(1)XO
03.1.1SG	15.0(1)XO1
03.2.0SG	15.0(2)SG
03.3.0SG	15.1(1)SG
03.3.1SG	15.1(1)SG1

Limitations and Restrictions

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

- More than 16K QoS policies can be configured in software. Only the first 16K are installed in hardware.
- Adjacency learning (through ARP response frames) is restricted to roughly 1000 new adjacencies per second, depending on CPU utilization. This should only impact large networks on the first bootup. After adjacencies are learned they are installed in hardware.

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

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

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

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

  Workaround (1):

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

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

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

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

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

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

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

  will produce the following for the first and second rules

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

  and the following for the third statement

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

Workaround (2):

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

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

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

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

CSCtg93278

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

  Workaround: None. CSCtr51014
- When OSPFv3 LSA throttling is configured, rate limiting does not take effect for a few minutes.

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

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

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

  Workaround: None. CSCty79236
- Auto negotiation cannot be disabled on the Fa1 port. It must be set to auto/auto, or fixed speed with duplex auto.

Caveats

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

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

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

Open Caveats for Cisco IOS XE Release 3.3.2SG

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

- On a Catalyst 4500 series switch, running Cisco IOS-XE Release 03.03.2SG, QoS service policies are applied on VLANs where the user has not configured this.

  For example, if a Catalyst 4500 series switch has two groups of VLANs defined in VLAN configuration mode:

  - A- 1 group only has QoS defined
  - B- 1 group only has Netflow defined

  When you enter the VLAN configuration mode for a VLAN that belongs to group A and configure the same NetFlow policy present in group B, ALL group B VLANs inherit the QoS configuration, even if you do not apply it.

  The problem is seen only on a Catalyst 4500 series switch, running Cisco IOS-XE Release 03.03.2SG

  Workaround: None. CSCus20676

- 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

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

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

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

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

  CSCto27085

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

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

- 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

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

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

  Workaround: None. CSCtu37959

- On a redundant system consisting of Supervisor Engine 6-E and Supervisor Engine 7-E, when the system uses considerable memory (for example, with heavy multicast traffic), a crash may occur. This event is due to a memory mismatch between the two supervisor engines.

  Workaround: Upgrade the memory of the Supervisor Engine 6-E to match that of the Supervisor Engine 7-E.

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

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

- 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

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

  Workaround: None. CSCtx95359
- 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
- A switch running a Supervisor Engine 7-E or Supervisor Engine 7L-E fails if you enter **show memory debug leak** on the console while **show memory detailed process iosd debug leaks** is being executed from another Telnet session.

  Workaround: Avoid running both commands simultaneously. CSCty27680
- If a configuration contains an "ip vrf" or "vrf definition" section, and you type “wr mem” while using an IP Base or LAN Base boot level of IOS-XE, the following message appears.

  Workaround: None. The message is information only. CSCtw93140
- With IGMP snooping enabled, multicast traffic received through a tunnel interface is not forwarded out the Outgoing Interface List.

  Workaround: Disable IGMP snooping. CSCuc65538
- 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

Resolved Caveats for Cisco IOS XE Release 3.3.2SG

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

- After booting a switch with Cisco IOS XE 3.3.0SG or 3.3.1SG with a crypto (k9) image, a linecard may display a status of Auth Fail, and will not be brought online. Non-crypto images are unaffected.

  Workaround: Reset the linecard either with the **hw-module module** *m* **reset** command or through a manual OIR. CSCuc64146

Open Caveats for Cisco IOS XE Release 3.3.1SG

This section lists the open caveats for Cisco IOS XE Release 3.3.1SG:

- 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

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

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

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

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

  CSCto27085

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

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

- 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

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

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

  Workaround: None. CSCtu37959

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

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

- 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

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

  Workaround: None. CSCtx95359

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

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

- When MLD Snooping is disabled, a Catalyst 4500X Series switches cannot maintain six MLD joins. This causes traffic loss due to missing outgoing interfaces.

  Workaround: Enable MLD snooping. CSCtx82176

- If a switch enabled with Bidir PIM has a software tunnel interface pointing towards the RP upstream, packet drops are observed.

  Workaround: None. Consider using a physical interface pointing towards RP upstream.

  CSCtz11352

- 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

- A WS-C4500X Series switch will fail when you use the **switchport** command to convert ports from Layer 3 to Layer 2, if the former is configured with IPv4 and IPv6 ACLs (each with 500 ACEs).

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

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

  Workaround:the 4500X uplink module by first pressing the ejector button for 10 seconds until the light turns green. CSCty67871

  Caution: the module without following this procedure is unsupported and will always produce a crash. To avoid the potential for black-holing traffic, use the ejector button.

- For the Ten-Gigabit interface on a C4500X switch, link flaps are observed if the debounce interval is defined with the **link debounce time** command to within 1 sec of the pulse interval.

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

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

- A C4500X switch fails if you enter **show memory debug leak** on the console while **show memory detailed process iosd debug leaks** is being executed from another Telnet session.

  Workaround: Avoid running both commands simultaneously. CSCty27680

- A switch running Cisco XE 3.3.0SG crashes when you use SPAN.

  Workaround: None. CSCua12869

- If a configuration contains an "ip vrf" or "vrf definition" section, and you type “wr mem” while using an IP Base or LAN Base boot level of IOS-XE, the following message appears.

  Workaround: None. The message is information only. CSCtw93140

- After logging “Authorization succeeded for client (Unknown MAC)” , a switch crashes if the following conditions apply:

  - A switchport is configured with both of the following:

    authentication event server dead action authorize...

    authentication event server alive action reinitalize

  - The RADIUS server was down previously, and a port without traffic (for example: a hub with no devices attached) was authorized into the inaccessible authentication bypass (IAB) VLAN without an associated MAC address.

  - The RADIUS server becomes available again, and a dot1x client attempts to authenticate.

  Workaround: None. CSCtx61557

- Traffic is dropped on a particular tx-queue of an EtherChannel member interfacere configured with a queuing policy. However, it will still appear in an egress span session of the EtherChannel.

  The **show platform software interface tx-queue** command will display an incorrect number of configured queues (compare to EtherChannel members that are not dropping traffic).

  Workaround: Enter shut then no shut on the port. CSCua66962

- On a switch running Cisco XE 3.2.4SG or 3.3.0SG with 4648* or 4748* linecards with PoE, a single port on a linecard fails to link up, usually after flapping its link frequently.

  Workaround: Enter **shut** then **no shut** on the port. CSCtz94862

- On a switch running Cisco XE 3.2.4SG or 3.3.0SG on 4648* or 4748* linecards with PoE, the PoE device will not power up on a single port, but will work on other ports on the same linecard.

  Workarounds:

  - Connect a non-PoE device to the port

  - Enter shut then no shut on the port. CSCua63562
- While running flexible netflow, the extended VLAN range of 1024-4000 is not observed in the software cache flow.

  Workaround: None CSCtz95537
- When a QoS policy is attached to a physical interface on a module or to a channel port containing interfaces on the module, a crash may occur when you remove a line card.

  Workaround: Remove the QoS policy before removing the linecard. CSCtz39815
- Front panel power supply LEDs do not always correspond to power supply state.

  Workaround: None. CSCtz01430
- UDE does not function at 1Gbps.

  Workaround: None. CSCuj56314

Resolved Caveats for Cisco IOS XE Release 3.3.1SG

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

- MAC addresses are not learned on dot1q-tunnel ports for transported VLAN MACs.

  Workaround: None. CSCub01918

Open Caveats for Cisco IOS XE Release 3.3.0SG

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

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

  Workaround: Enter **shut** and **no shut** on the port to synchronize the STP state. CSCtf52437
- If you reboot a switch, the configured value of the interface MTU size for the elements of the port channel interface does not work for IPv6 traffic.

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

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

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

- 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

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

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

  Workaround: None. CSCtu37959

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

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

- 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

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

  Workaround: None. CSCtx95359

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

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

- When MLD Snooping is disabled, a C4500X switch cannot maintain six MLD joins. This causes traffic loss due to missing outgoing interfaces.

  Workaround: Enable MLD snooping. CSCtx82176

- If a switch enabled with Bidir PIM has a software tunnel interface pointing towards the RP upstream, packet drops are observed.

  Workaround: None. Consider using a physical interface pointing towards RP upstream.

  CSCtz11352

- 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

- A C4500X switch will fail when you use the **switchport** command to convert ports from Layer 3 to Layer 2, if the former is configured with IPv4 and IPv6 ACLs (each with 500 ACEs).

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

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

  Workaround:the 4500X uplink module by first pressing the ejector button for 10 seconds until the light turns green. CSCty67871

  Caution: the module without following this procedure is unsupported and will always produce a crash. To avoid the potential for black-holing traffic, use the ejector button.

- For the Ten-Gigabit interface on a C4500X switch, link flaps are observed if the debounce interval is defined with the **link debounce time** command to within 1 sec of the pulse interval.

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

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

- A C4500X switch fails if you enter **show memory debug leak** on the console while **show memory detailed process iosd debug leaks** is being executed from another Telnet session.

Workaround: Avoid running both commands simultaneously. CSCty27680

- MAC addresses are not learned on dot1q-tunnel ports for transported VLAN MACs.

  Workaround: None. CSCub01918
- UDE does not function at 1Gbps.

  Workaround: None. CSCuj56314

Resolved Caveats for Cisco IOS XE Release 3.3.0SG

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

- If you enter the **show spanning-tree vlan** command when spanning tree is changed from PVST to Rapid PVST, the ports configured as promiscuous trunks are not listed as part of the spanning tree.

  Workaround: Enter **shut** and **no shut** on the ports. CSCtn88228
- If you enter the **show mem detailed process ?** command on a Supervisor Engine 7-E switch, a list of processes is not displayed.

  Workaround: Enter the complete command string, for example:

  ```
  show mem detailed process cli_agent
  ```

  CSCtj05663
- If you enter the **clear ip mroute ?** command, only the **vrf** option is displayed. The **Hostname** and ' * ' options are not displayed, even though they are accepted by the system. The **clear ip mroute** command functions as expected.

  Workaround: None. CSCto59368

Troubleshooting

These sections provide troubleshooting guidelines for the Catalyst 4500 series switches:

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-universalk9.03.03.00 .SG.151-1.SG .bin located on the TFTP server 172.16.1.8, enter the following command:

```
rommon 3> boot tftp://172.16.1.8/tftpboot/cat4500e-universalk9.03.03.00
.SG.151-1.sg.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

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:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Original SSLeay License:

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

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

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

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

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

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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

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

Release Notes for the Catalyst 4500E Series Switch, Cisco Release IOS XE 3.2.X SG