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

IOS XE 3.2.11SG—October 18, 2016

Prior Release
IOS XE 3.2.10SG, IOS XE 3.2.9SG, IOS XE 3.2.8SG, IOS XE 3.2.7SG, IOS XE 3.2.6,SG IOS XE 3.2.5SG, IOS XE 3.2.4SG, IOS XE 3.2.3SG, IOS XE 3.2.2SG, IOS XE 3.2.1SG, IOS XE 3.2.0SG

This release note describes the features, modifications, and caveats for the Cisco IOS XE 3.2.0SG software on the Catalyst 4500E series switch with Supervisor Engine 7-E.

Cisco IOS XE Software Release 3.1.0 SG introduced primary hardware and software innovations including:

- Support for next-generation Cisco® Catalyst® 4500E Series system Supervisor Engine 7-E and associated line cards
- Deep application and security visibility and policy controls with Flexible Netflow and Embedded Event Manager (EEM) integration
- Extensible operating system with Cisco IOS XE Software
- Simplified software management and compliance audit with Cisco software activation licensing

Support for Cisco IOS XE Release 3.2.0SG, 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 Catalyst 4500E series switches, 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 for IOS 3.2.xSG

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 and Enhanced Interior Gateway Routing Protocol (EIGRP) "limited" Stub Routing, and RIPv1/v2. The IP Base image does not support enhanced routing features such as Nonstop Forwarding/Stateful Switchover (NSF/SSO), BGP, Intermediate System-to-Intermediate System (IS-IS), Internetwork Packet Exchange (IPX), AppleTalk, Virtual Routing Forwarding (VRF-lite), GLBP, and policy-based routing (PBR).

LAN Base image is primarily 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 XE 3.2.0SG, support for HSRP v2 IPV6 has 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 4500E Supervisor Engine 7-E running Cisco IOS Software Release 3.2.0SG categorized by image type. Please visit Feature Navigator for package details:

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

Table 1 LAN Base/IP Base/EnterpriseServices Image Support on Cisco Catalyst 4500E Supervisor Engine 7-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 Sequence Numbering	Yes	Yes	Yes
Address Resolution Protocol (ARP)	Yes	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-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 Multipath Support	No	No	Yes
BGP 4 Prefix Filter and In-bound Route Maps	No	No	Yes
BGP 4 Soft Config	No	No	Yes
BGP Conditional Route Injection	No	No	Yes
BGP Configuration Using Peer Templates	No	No	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
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
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
CGMP - Cisco Group Management Protocol	No	Yes	Yes
Cisco IOS Scripting w/Tel	Yes	Yes	Yes
Cisco TrustSec SGT Exchange Protocol (SXP) IPv4	No	Yes	Yes
CiscoView Autonomous Device Manager (ADP)	No	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
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
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

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

Feature	LAN Base	IP Base	Enterprise Services
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
DHCP 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
Duplication Location Reporting Issue	No	Yes	Yes
Dynamic Trunking Protocol (DTP)	Yes	Yes	Yes
EIGRP	No	No	Yes
EIGRP Stub Routing	No	Yes	Yes
Embedded Event Manager (EEM) 3.2	No	Yes	Yes
Embedded Syslog Manager (ESM)	Yes	Yes	Yes
EnergyWise	Yes	Yes	Yes
Enhanced PoE Support (Additional Wattage Range)	Yes	Yes	Yes
Entity API for Physical and Logical Mgd Entities	Yes	Yes	Yes
ErrDisable timeout	Yes	Yes	Yes
EtherChannel	Yes	Yes	Yes
EtherChannel Flexible PAgP	Yes	Yes	Yes
EtherChannel Single Port Channel	Yes	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
Fast EtherChannel (FEC)	Yes	Yes	Yes
FHRP - Enhanced Object Tracking of IP SLAs	No	Yes	Yes
FHRP EOT 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
Microflow policers	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 - Netflow Export over IPv4	No	Yes	Yes
Flexible Netflow - Netflow v9 Export Format	No	Yes	Yes
Flexible Netflow - Multiple User Defined Caches	No	Yes	Yes
Flexible Netflow - NetflowV5 export protocol	No	Yes	Yes
Flexible Netflow - Full Flow support	No	Yes	Yes
Forced 10/100 Autonegotiation	Yes	Yes	Yes
FTP Support for Downloading Software Images	Yes	Yes	Yes
Gateway Load Balancing Protocol GLBP	No	Yes	Yes
Generic Routing Encapsulation (GRE) Tunneling in software	No	Yes	Yes
HSRP - Hot Standby Router Protocol	No	Yes	Yes
HTTP Security	Yes	Yes	Yes
HTTP TACAC+ Accounting support	No	No	Yes
IEEE 802.1ab LLDP (Link Layer Discovery Protocol)	Yes	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
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 VLAN Assignment	Yes	Yes	Yes
IEEE 802.1x Wake on LAN Support	Yes	Yes	Yes
IEEE 802.1x Authenticator	Yes	Yes	Yes
IEEE 802.1x Fallback support	Yes	Yes	Yes
IEEE 802.1x Guest VLAN	Yes	Yes	Yes
IEEE 802.1X Multi-Domain Authentication	Yes	Yes	Yes
IEEE 802.1x Private Guest VLAN	Yes	Yes	Yes
IEEE 802.1x Private VLAN Assignment	Yes	Yes	Yes
IEEE 802.1x RADIUS Accounting	Yes	Yes	Yes
IEEE 802.1x RADIUS-Supplied Session Timeout	Yes	Yes	Yes
IEEE 802.1X with ACL Assignments	Yes	Yes	Yes
IEEE 802.1X with Port Security	Yes	Yes	Yes
IEEE 802.3ad Link Aggregation (LACP)	Yes	Yes	Yes
IEEE 802.3ad Link Aggregation (LACP) Port-Channel Standalone Disable	Yes	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
IEEE 802.3af PoE (Power over Ethernet)	Yes	Yes	Yes
IEEE 802.3x Flow Control	Yes	Yes	Yes
IGMP Fast Leave	Yes	Yes	Yes
IGMP Filtering	Yes	Yes	Yes
IGMP Snooping	Yes	Yes	Yes
IGMP Version 1	Yes	Yes	Yes
IGMP Version 2	Yes	Yes	Yes
IGMP Version 3	Yes	Yes	Yes
IGMP Version 3 - Explicit Tracking of Hosts, Groups, and Channels	Yes	Yes	Yes
IGMPv3 Snooping: Full Support	Yes	Yes	Yes
Image Verification	Yes	Yes	Yes
Individual SNMP Trap Support	Yes	Yes	Yes
Inline Power Auto Negotiation	Yes	Yes	Yes
Inline Power Management	Yes	Yes	Yes
Interface Index Persistence	Yes	Yes	Yes
Interface Range Specification	Yes	Yes	Yes
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
IP over IPv6 Tunnels	No	Yes	Yes
IP Routing	Yes	Yes	Yes
IP SLAs - DHCP Operations	No	No	Yes
IP SLAs - Distribution of Statistics	No	No	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
IP SLAs - DNS Operation	No	No	Yes
IP SLAs - FTP Operation	No	No	Yes
IP SLA - HTTP Operation	No	No	Yes
IP SLAs-ICMP Echo Operation	No	No	Yes
IP SLAs - ICMP Path Echo Operation	No	No	Yes
IP SLAs - Multi Operation Scheduler	No	No	Yes
IP SLAs - One Way Measurement	No	No	Yes
IP SLAs - Path Jitter Operation	No	No	Yes
IP SLAs - Reaction Threshold	No	No	Yes
IP SLAs - Scheduler	No	No	Yes
IP SLAs - TCP Connect Operation	No	No	Yes
IP SLAs - UDP Based VoIP Operation	No	No	Yes
IP SLAs - UDP Echo Operation	No	No	Yes
IP SLAs - UDP Jitter Operation	No	No	Yes
IP SLAs - VoIP Threshold Traps	No	No	Yes
IP SLAs Random Scheduler	No	No	Yes
IP SLAs Responder	No	Yes	Yes
IP SLAs Sub-millisecond Accuracy Improvements	No	No	Yes
IP Summary Address for RIPv2	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

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

Feature	LAN Base	IP Base	Enterprise Services
IPv6 HTTP(S)	Yes	Yes	Yes
IPv6 IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	No	No	Yes
IPv6 - TCL	Yes	Yes	Yes
IPv6 (Internet Protocol Version 6)	Yes	Yes	Yes
IPv6 Access Services: DHCPv6 Relay Agent	No	No	Yes
IPv6 MLD Snooping v1 and v2	Yes	Yes	Yes
IPv6 MTU Path Discovery	Yes	Yes	Yes
IPv6 Multicast	No	Yes	Yes
IPv6 Multicast: Bootstrap Router (BSR)	No	No	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 Routing - EIGRP Support	No	No	Yes
IPv6 Routing: OSPF for IPv6 (OSPFv3)	No	No	Yes
IPv6 Routing: RIP for IPv6 (RIPng)	No	Yes	Yes
IPv6 Routing: Route Redistribution	No	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
IPv6 Routing: Static Routing	Yes	Yes	Yes
IPv6 Security: Secure Shell SSH support over IPv6	Yes	Yes	Yes
IPv6 Services: AAAA DNS Lookups over an IPv4 Transport	No	Yes	Yes
IPv6 Services: Cisco Discovery Protocol (CDP) - IPv6 Address Family Support for Neighbor Information	Yes	Yes	Yes
IPv6 Services: DNS Lookups over an IPv6 Transport	Yes	Yes	Yes
IPv6 Services: Extended Access Control Lists	Yes	Yes	Yes
IPv6 Services: Standard Access Control Lists	Yes	Yes	Yes
IPv6 Stateless Auto-configuration	Yes	Yes	Yes
IPv6 Switching: CEF Support	No	Yes	Yes
IPv6 Switching: CEFv6 Switched Automatic IPv4-compatible Tunnels	No	Yes	Yes
IPv6 Switching: CEFv6 Switched Configured IPv6 over IPv4 Tunnels	No	Yes	Yes
IPv6 Switching: CEFv6 Switched ISATAP Tunnels	No	Yes	Yes
IPv6 Tunneling: Automatic 6to4 Tunnels	No	Yes	Yes
IPv6 Tunneling: Automatic IPv4-compatible Tunnels	No	Yes	Yes
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	No	Yes	Yes
IPv6 Tunneling: ISATAP Tunnel Support	No	Yes	Yes
IPv6 Tunneling: Automatic IPv4-compatible Tunnels	No	Yes	Yes
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	No	Yes	Yes
IPv6 Tunneling: ISATAP Tunnel Support	No	Yes	Yes
IPv6 Tunneling: Manually Configured IPv6 over IPv4 Tunnels	No	Yes	Yes
IPv6: Anycast Address	Yes	Yes	Yes
IPv6: ICMPv6	Yes	Yes	Yes
IPv6: ICMPv6 Redirect	Yes	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
IPv6: Neighbor Discovery Duplicate Address Detection	Yes	Yes	Yes
ISSU (IOS In-Service Software Upgrade)	No	Yes	Yes
Jumbo Frames	Yes	Yes	Yes
Layer 2 Traceroute	No	Yes	Yes
Layer 3 Multicast Routing (PIM SM, SSM, Bidir)	No	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 for Voice VLAN	Yes	Yes	Yes
MAC Address Notification	Yes	Yes	Yes
MAC Authentication Bypass	Yes	Yes	Yes
Memory Threshold Notifications	Yes	Yes	Yes
Modular QoS CLI (MQC)	Yes	Yes	Yes
Multi-authentication and VLAN Assignment	Yes	Yes	Yes
Multi-VRF Support (VRF lite)	No	No	Yes
Multicast BGP (MBGP)	No	No	Yes
Multicast Fast Switching Performance Improvement	No	Yes	Yes
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
NETCONF over SSHv2	Yes	Yes	Yes
Network Time Protocol (NTP)	Yes	Yes	Yes
Network Time Protocol (NTP) primary (formerly known as Network Time Protocol (NTP) master)	Yes	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
No. of VLAN Support	2048	4096	4096
NSF - BGP	No	No	Yes
NSF - EIGRP	No	No	Yes
NSF - OSPF v2	No	No	Yes
NSF/SSO (Nonstop Forwarding with Stateful Switchover)	No	Yes	Yes
Onboard Failure Logging (OBFL)	Yes	Yes	Yes
OSPF	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[3]	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
Per Port Per VLAN Policing	Yes	Yes	Yes
Per-User ACL Support for 802.1X/MAB/Webauth users	Yes	Yes	Yes
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

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

Feature	LAN Base	IP Base	Enterprise Services
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
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
Rapid PVST+ Dispute Mechanism	Yes	Yes	Yes
Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)	Yes	Yes	Yes
Reduced MAC Address Usage	Yes	Yes	Yes
Redundancy Facility Protocol	Yes	Yes	Yes
Remote SPAN (RSPAN)	Yes	Yes	Yes
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

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

Feature	LAN Base	IP Base	Enterprise Services
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
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

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

Feature	LAN Base	IP Base	Enterprise Services
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
SVI (Switch Virtual Interface) Autostate Exclude	Yes	Yes	Yes
Switch and IP Phone Security Interaction	Yes	Yes	Yes
Switch Port Analyzer (SPAN)	Yes	Yes	Yes
Switch Port Analyzer (SPAN) - CPU Source	Yes	Yes	Yes
Syslog over IPV6	Yes	Yes	Yes
System Logging - EAL4 Certification Enhancements	No	Yes	Yes
Tacacs SENDAUTH function	Yes	Yes	Yes
Tacacs Single Connection	Yes	Yes	Yes
TACACS+	Yes	Yes	Yes
TCAM4 - Dynamic Multi-Protocol	Yes	Yes	Yes
TCAM4 - Service-Aware Resource Allocation	Yes	Yes	Yes
Time Domain Reflectometry (TDR)	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
UDI - Unique Device Identifier	Yes	Yes	Yes

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

Feature	LAN Base	IP Base	Enterprise Services
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
VLAN Access Control List (VACL)	Yes	Yes	Yes
VLAN MAC Address Filtering	Yes	Yes	Yes
VTP (Virtual Trunking Protocol) Version 2	Yes	Yes	Yes
VTP version 3	Yes	Yes	Yes
Web Authentication Proxy	Yes	Yes	Yes
Webauth Enhancements	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. 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 4500E Series Switch

The following features are not supported on a Catalyst 4500E Series Switch with Supervisor Engine 7-E:

- 802.3ah
- ANCP
- Autosmartport
- CBQoS MIB
- Cisco Network Assistant
- CISCO-IETF-IP-FORWARD-MIB
- CISCO-IETF-IP-MIB
- Flex Links+(VLAN Load balancing)

- HOT Ice
- ID4.1 802.1X User Distribution
- IP4.1 ACL Policy Enhancements
- IP4.1 MAC MOve and Replace
- IP4.1 NEAT
- IP4.1 RADIUS CoA
- IPSG for Static Hosts
- IPUnnumbered
- IPv6 Intf Stats and MIB
- IPv6 PACL and RACL
- IPv6 RA Guard (host mode only)
- IS-IS v4, v6
- Layer 2 Control Packet QoS
- Link Debug
- Link State Tracking
- LLDP HA
- LLDP MED MIB
- Management Port
- NMSP
- PPPoE
- PVL
- QnQ and L2PT
- REP
- Subsecond UDLD
- SwQoS
- TACACS Aware VRF
- VLAN Translation
- WCCP Version
- Y.1731 (AIS and RDI)

Orderable Product Numbers

Table 2 Cisco IOS Software Release 3.2.0SG Product Numbers and Images

Product Number	Description	Image
S45U-32-1502SG	CAT4500e SUP7e Universal Image	cat4500e-universal.SPA.03.02.00.SG.150-2.SG.bin

Table 2 Cisco IOS Software Release 3.2.0SG Product Numbers and Images

Product Number	Description	Image
S45UK9-32-1502SG	CAT4500e SUP7e Universal Crypto Image	cat4500e-universalk9.SPA.03.02.00.SG.150-2.SG.bin
C4500E-LIC=	Base product ID for paper delivered software licenses	NA
C4500E-LB	LAN BASE software license (paper delivery)	NA
C4500E-IPB	IP BASE software license (paper delivery)	NA
C4500E-LB-IPB	LAN BASE to IP BASE upgrade license (paper delivery)	NA
C4500E-LB-ES	LAN BASE to Enterprise Services upgrade license (paper delivery)	NA
C4500E-IP-ES	IP BASE to Enterprise Services upgrade license (paper delivery)	NA
C4500E-LIC-PAK	Base product ID for paper delivered software licenses for spare Supervisor Engine 7-E	NA
C4500E-IP-ES-S	IP BASE to Enterprise Services upgrade license for spare Supervisor Engine7-E(paper delivery)	NA
C4500E-IPB-S	IP BASE software license for spare Supervisor Engine 7-E (paper delivery)	NA
L-C4500-LIC=	Base product ID for electronically delivered software licenses	NA
L-C4500E-LB-IP	LAN BASE to IP BASE upgrade license (electronically delivered)	NA
L-C4500E-IP-ES	IP BASE to Enterprise Services upgrade license (electronically delivered)	NA
L-C4500E-LB-ES	LAN BASE to Enterprise Services upgrade license (electronically delivered)	NA

Catalyst 4500E Series Switch Cisco Classic IOS XE Release Strategy

Note These recommendations are up to date at the time of release note publications. For the latest recommendations, please consult the release notes for the most recent software version supporting this hardware.

Cisco IOS Release 3.2.0 train offers the latest features for the Catalyst 4500 Supervisor Engine 7-E. If you need to need the latest hardware support and software features you should migrate to Cisco IOS Release 3.2.0SG.

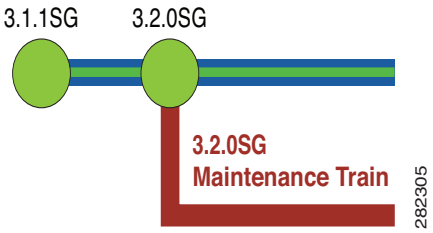
For more information on the Catalyst 4500 series switches, visit the following URL:

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

Cisco IOS Software Migration Guide

Figure 1 displays the one active train, 3.2.0SG.

Figure 1 Software Release Strategy for the Catalyst 4500 Series Switch



Summary of Migration Plan

Customers requiring the latest Cisco Catalyst 4500 Series hardware and software features should migrate to Cisco IOS Software Release 3.2.0SG, which will be an extended maintenance release.

Support

Support for Cisco IOS Software Release 15.0(2)SG follows the standard Cisco Systems® support policy, available at
http://www.cisco.com/en/US/products/products_end-of-life_policy.html

Support

Support for Cisco IOS Software Release 3.2.0SG follows the standard Cisco Systems® support policy, available at

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

System Requirements

This section describes the system requirements:

Supported Hardware on the Catalyst 4500E Series Switch

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

Table 3 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 7-E

Product Number (append with "=" for spares)	**Product Description**
Supervisor Engines	
WS-X45-Sup7-E	Catalyst 4500E-series switch Supervisor Engine 7-E **Note** This engine is supported on E-series, R-E, and R+E chassis.
10 Gigabit Ethernet Switching Modules	
WS-X4712-SFP+E	12-port 10 Gigabit Ethernet (SFP+) line card Not supported on 4507R-E and 4510R-E chassis.
WS-X4606-X2-E	6-port X2 line card
Gigabit Ethernet Switching Modules	
WS-X4302-GB	2-port 1000BASE-X (GBIC) Gigabit Ethernet module
WS-X4306-GB	6-port 1000BASE-X (GBIC) Gigabit Ethernet switching module
WS-X4418-GB	18-port 1000BASE-X (GBIC) Gigabit Ethernet server switching module
WS-X4412-2GB-T	12-port 1000BASE-T Gigabit Ethernet and 2-GBIC ports switching module
WS-X4424-GB-RJ45	24-port 10/100/1000BASE-T Gigabit Ethernet RJ-45 switching module
WS-X4448-GB-LX	48-port 1000BASE-LX (small form-factor pluggable) Gigabit Ethernet fiber optic interface switching module
WS-X4448-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet switching module
WS-X4448-GB-SFP	48-port 1000BASE-X (small form-factor pluggable) module

Table 3 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 7-E (continued)

Product Number (append with "=" for spares)	**Product Description**
WS-X4506-GB-T	6-port Alternately-Wired 10/100/1000BASE-T Catalyst 4500 series Power over Ethernet (PoE) 802.3af or 1000BASE-X SFP
WS-X4524-GB-RJ45V	24-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af
WS-X4548-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet module
WS-X4548-GB-RJ45V	48-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af
WS-X4548-RJ45V+	48-port 10/100/1000 Premium PoE line card
WS-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-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-X4648-RJ45-E	48 port 10/100/1000BT with 2 to 1 oversubscription and jumbo frame support
WS-X4648-RJ45V-E	48 port 10/100/1000 Mb with 2 to 1 oversubscription PoE 802.3af providing up to 20 Watts power/port
WS-X4648-RJ45V+E	48 port 10/100/1000 Mb with 2 to 1 oversubscription PoE 802.3at providing up to 30 Watts power/port
WS-X4748-RJ45V+E	48-port 10/100/1000 line card nonblocking PoE 802.3at providing up to 30 Watts power/port
WS-X4748-UPOE+E	48-port 10/100/1000 line card nonblocking PoE 802.3at and 60 watt UPoE PoE linecard with Ethernet Energy Efficient feature.
WS-X4748-RJ45-E	48-port 10/100/1000 nonblocking line card with the Ethernet Energy Efficient feature
Fast Ethernet Switching Modules	
WS-X4124-FX-MT	24-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module
WS-X4148-FX-MT	48-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module
WS-X4148-FE-LX-MT	48-port 100BASE-LX10 Fast Ethernet MT-RJ single-mode fiber switching module
WS-X4148-FE-BD-LC	48-port 100BASE-BX10-D module
WS-X4248-FE-SFP	48-port 100BASE-X SFP switching module
WS-U4504-FX-MT	4-port 100BASE-FX (MT-RF) uplink daughter card
Ethernet/Fast Ethernet (10/100) Switching Modules	
WS-X4124-RJ45	24-port 10/100 RJ-45 module
WS-X4148-RJ	48-port 10/100 RJ-45 switching module
WS-X4148-RJ21	48-port 10/100 4xRJ-21 (telco connector) switching module
WS-X4148-RJ45V	48-port Pre-standard PoE 10/100BASE-T switching module
WS-X4224-RJ45V	24-port 10/100BASE-TX RJ-45 Cisco Catalyst 4500 series PoE 802.3af
WS-X4232-GB-RJ	32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet switching module
WS-X4248-RJ45V	48-port 10/100BASE-T RJ-45 Cisco Catalyst 4500 series PoE 802.3af
WS-X4248-RJ21V	48-port 10/100 Fast Ethernet RJ-21 Cisco Catalyst 4500 series PoE 802.3af telco

Table 3 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 7-E (continued)

Product Number (append with "=" for spares)	**Product Description**
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-100FX	100BASE-FX, 1310 nm wavelength, 2 km over MMF
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
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 27.
GLC-BX-U	1000BASE-BX10-U small form-factor pluggable module For DOM support, see Table 6 on page 27.bv
GLC-SX-MM	1000BASE-SX small form-factor pluggable module
GLC-LH-SM	1000BASE-LX/LH small form-factor pluggable module
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 25 for a list of supported wavelengths.) For DOM support, see Table 6 on page 27.
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

Table 3 Supported Hardware on Cisco Catalyst 4500E Supervisor Engine 7-E (continued)

Product Number (append with "=" for spares)	**Product Description**
SFP-H10GB-CU5M	10GBASE-CU SFP+ Cable 5 Meter
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 25 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 27.
WDM-GBIC-REC	Receive-only 1000BASE-WDM GBIC
Other Modules	
MEM-X45-2GB-E	SD Card, 2G
USB-X45-4GB-E	USB Thumb Drive, 4G
PWR-C45-1000AC	Catalyst 4500 series switch 1000 Watt AC power supply for chassis 4503, 4506, and 4507R (data only)
PWR-C45-1400DC	Catalyst 4500 series switch 1400 Watt DC triple input power supply (data-only)
PWR-C45-1400DC-P	Catalyst 4500 series switch 1400 Watt DC power supply with integrated PEM
PWR-C45-1400AC	Catalyst 4500 series switch 1400 Watt AC power supply (data-only)
PWR-C45-1300ACV	Catalyst 4500 series switch 1300 Watt AC power supply with integrated voice for chassis 4503, 4506, and 4507R
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 4 CWDM GBIC and SFP Supported Wavelengths on Cisco Catalyst 4500E Supervisor Engine 7-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

Table 4 CWDM GBIC and SFP Supported Wavelengths on Cisco Catalyst 4500E Supervisor Engine 7-E

Product Number (append with "=" for spares)	**Product Description**
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 briefly describes the supported DWDM wavelengths in the Catalyst 4500E Series Switch.

Table 5 DWDM SFP Supported Wavelengths on Cisco Catalyst 4500E Supervisor Engine 7-E

Product Number (append with "=" for spares)	**Product Description**
DWDM-SFP-6061=	Cisco 1000BASE-DWDM SFP 1560.61 nm
DWDM-SFP-5979=	Cisco 1000BASE-DWDM SFP 1559.79 nm
DWDM-SFP-5898=	Cisco 1000BASE-DWDM SFP 1558.98 nm
DWDM-SFP-5817=	Cisco 1000BASE-DWDM SFP 1558.17 nm
DWDM-SFP-5655=	Cisco 1000BASE-DWDM SFP 1556.55 nm
DWDM-SFP-5575=	Cisco 1000BASE-DWDM SFP 1555.75 nm
DWDM-SFP-5413=	Cisco 1000BASE-DWDM SFP 1554.13 nm
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

Table 5 DWDM SFP Supported Wavelengths on Cisco Catalyst 4500E Supervisor Engine 7-E

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

SFP	GLC-BX-D
SFP	GLC-BX-U
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 3.2.0SG

Cisco IOS XE Release 3.2.0SG supports the next-generation high-performance E Series Supervisor Engine 7-E with CenterFlex technology and E-Series line cards and chassis. A brief list of primary E-Series hardware supported by Cisco IOS XE Release 3.2.0SG 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
WS-C4506-E	Cisco Catalyst 4500E Series 6-Slot Chassis • Fan tray • No Power Supply
WS-C4507R-E	Cisco Catalyst 4500E Series 7-Slot Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 3 and/or 4; the backplane will enforce this restriction.
WS-C4507R+E	Cisco Catalyst 4500E Series 7-Slot 48 GB-ready Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 3 and/or 4; the backplane will enforce this restriction.
WS-C4510R-E	Cisco Catalyst 4500E Series 10-Slot Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 5 and/or 6; the backplane will enforce this restriction.
WS-C4510R+E	Cisco Catalyst 4500E Series 10-Slot 48 GB-ready Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • In this chassis, supervisor engines must sit in slots 5 and/or 6; the backplane will enforce this restriction.

New and Changed Information

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

- New Software Features in Release IOS XE 3.2.1SG, page 29

Note Release IOS XE 3.1.1 is a rebuild of Release IOS XE 3.1.0 with only 2 bug fixes included.

New Software Features in Release IOS XE 3.2.1SG

Release IOS XE 3.2.1SG provides the following new software on the Catalyst 4500 series switch:

- IEEE 802.3ad Link Aggregation (LACP) Port-Channel Standalone Disable

New Hardware Features in Release IOS XE 3.2.1SG

Release IOS XE 3.2.1SG provides the following new hardware on the Catalyst 4500 series switch.

- WS-X4640-CSFP-E

New Software Features in Release IOS XE 3.2.0SG

Release IOS XE 3.2.0SG provides the following new software on the Catalyst 4500 series switch:

- 2-way Community Private VLANs ("Configuring Private VLANs" chapter)
- Call Home message using dedicated interface (“Configuring Call Home” chapter)
- CPU Optimization for Layer 3 Multicast Control Packets (“Configuring Network Security with ACLs” chapter)
- Critical Authorization for Voice and Data (“Configuring 802.1X Port-Based Authentication 802.1X” chapter)
- Duplication Location Reporting Issue

  For information on the reporting issue, refer to the following URL:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover.html
- IEEE 802.1ag - D8.1 standard Compliant CFM, Y.1731 multicast LBM / AIS / RDI / LCK, IP SLA for Ethernet (“Configuring Ethernet OAM and CFM” chapter)
- Multi-authentication and VLAN Assignment (“Configuring 802.1X Port-Based Authentication 802.1X” chapter)
- Propagation of Location Info over CDP

  For information on configuring CDP Location TLV, refer to the following URL:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover.html
- PVLAN over EtherChannel ("Configuring Private VLANs" chapter)
- Support for 32k mroutes

New Hardware Features in Release IOS XE 3.2.0SG

Release IOS XE 3.2.0SG provides the following new hardware on the Catalyst 4500 series switch:

- SFP-10G-ER—10GBASE-ER SFP+ transceiver module for SMF, 1550-nm, LC duplex connector
- SFP-10G-ZR—10GBASE-ZR SFP+ transceiver module for SMF, 1550-nm, LC duplex connector
- DWDM SFP Transceivers (8 additional wavelengths) (dual LC/PC connector):
  - DWDM-SFP-6141= (Cisco 1000BASE-DWDM SFP 1561.42 nm)
  - DWDM-SFP-5736= (Cisco 1000BASE-DWDM SFP 1557.36 nm)
  - DWDM-SFP-5332= (Cisco 1000BASE-DWDM SFP 1553.33 nm)
  - DWDM-SFP-4931= (Cisco 1000BASE-DWDM SFP 1549.32 nm)
  - DWDM-SFP-4532= (Cisco 1000BASE-DWDM SFP 1545.32 nm)
  - DWDM-SFP-4134= (Cisco 1000BASE-DWDM SFP 1541.35 nm)
  - DWDM-SFP-3739= (Cisco 1000BASE-DWDM SFP 1537.40 nm)
  - DWDM-SFP-3346= (Cisco 1000BASE-DWDM SFP 1533.47 nm)
- WS-X4748-UPOE+E
- WS-X4748-RJ45-E

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
03.1.0SG	15.0(1)XO
03.1.1SG	15.0(1)XO1
03.2.0SG	15.0(2)SG

Upgrading the System Software

If you are upgrading to 3.2.0SG, you must upgrade your ROMMON to 15.0(1r)SG2.

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

If they have dual supervisors, first upgrade your software to 3.2.0SG, then upgrade your ROMMON to 15.0(1r)SG2 to avoid the resets uplinks issue (CSCtj54375).

Identifying an +E Chassis and ROMMON

An +E chassis is identified by a FRU minor value in the chassis' idprom.

When supervisor engine 1 (sup1) is in ROMMON and supervisor engine 2 (sup2) is in IOS, only sup2 can read the idprom contents of chassis' idprom. Chassis type is displayed as "+E" in the output of the **show version** command. Conversely, sup1 can only display the chassis type as "E."

When both sup1 and sup2 are in ROMMON, both engines can read the chassis' idprom. Chassis type is displayed correctly as "+E" in the output of the **show version** command.

When both sup1 and sup2 are in IOS, both engines can read the chassis' idprom. Chassis type is displayed correctly as "+E" in the output of the **show version** command.

Limitations and Restrictions

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

- The supervisor engine front-panel management port (FastEthernet1 interface) is not supported.
- The WS-X4712-SFP+E module is not supported in the WS-C4507R-E or WS-C4510R-E chassis and does not boot. This module is supported in the WS-C4503-E, WS-C4506-E, WS-C4507R+E, and WS-C4510R+E chassis.
- 802.1q tunneling and related features are not supported.
- 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.

- A switch crashes after displaying the message:

  ```
  %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
  MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
  ```

  provided the following conditions apply:

  – A switchport is configured with the following:

  authentication event server dead action authorize...

  authenticaton 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 the IAB-authorized port transitions to another state.

  Workaround: None. CSCtx61557

Caveats

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

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

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

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

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

1. Access the BST (use your Cisco user ID and password) at https://tools.cisco.com/bugsearch/.
2. Enter the bug ID in the **Search For:** field.

Resolved Caveats in Cisco IOS XE Release 3.2.11SG

Use the Bug Search Tool to view the details of a caveat listed in this section:

Table 9 Resolved Caveats in IOS XE Release 3.2.11SG

Bug ID	Headline
CSCts66733	Crash @ tftp_server
CSCup90532	memory corruption crash related to DNS
CSCut15649	GLC-BX-D is not being recognized with Sup V(WS-X4516-10GE)
CSCut87425	CPU hog in "EEM TCL Proc" after TCL script termination with long runtime
CSCuu18788	DATACORRUPTION-1-DATAINCONSISTENCY when polling ceExtSysBootImageList
CSCuu43892	switch crash on qpair_full after executing dhcpd_* functions
CSCuv36461	Memory leak at SPI iif reg(PC: 0xF64E0E91)
CSCuw48118	ASR920 - crash in bcopy called from 'addnew' during reassembly
CSCux65501	4500X forwards Ethernet I frames on stp blocked port
CSCux66005	ASR crash while handling fragmented traffic
CSCuy87667	Crash due to Block overrun by AAA banner
CSCuz08035	Software fix for DHM Parity error.
CSCuz26852	Interrupts for Parity Error are not enabled after 'reload' command.

Open Caveats for Cisco IOS XE Release 3.2.10SG

This section lists the open caveats for Cisco IOS XE Release 3.2.9SG:

- The Cisco IOS XE software for the Cisco Catalyst 4500 Series switches includes a version of Bash that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

  CVE-2014-6271

  CVE-2014-6277

  CVE-2014-6278

  CVE-2014-7169

  CVE-2014-7186

  CVE-2014-7187

  Cisco has analyzed this vulnerability and concluded that while the previously listed products may run a vulnerable version of Bash, there are no exploitation vectors present - therefore, those products are not impacted.

  Additional details about those vulnerabilities can be found at http://cve.mitre.org/cve/cve.html

  Workaround: None. CSCur03368

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

  This problem affects the Cisco Catalyst 4500 Series Supervisor 7E.

  Workaround: None. CSCth65129

- When either the RADIUS-server test feature or RADIUS-erver dead-criteria is configured and either RADIUS-server deadtime is not configured or is set to 0, 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 spanning tree is changed from PVST to Rapid PVST and you enter the **show spanning-tree vlan** command, the ports configured as promiscuous trunks are not listed as part of the spanning tree.

  Workaround: Enter **shut**, then **no shut** on the ports. CSCtn88228

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

  Workaround: None. CSCto59368

- On Supervisor Engine 7-E, DBL might not funciton 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 occurs 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 capable of 2nd-port-TLV, 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 linecard, several %C4K_RKNOVA-4-INVALIDTOKENEXPIRED messages appear in the logs.

  Workaround: None. CSCtu37959

- On a redundant system consisting of supervisor engines 6-E and 7-E, when the system consumes 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 Supervisor Engine 6-E to match that of Supervisor Engine 7-E.

- Configuring an interface as uni-directional 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 bi-directional mode.

  Workaround: None. CSCtx95359

Resolved Caveats in Cisco IOS XE Release 3.2.10SG

- Certain modules X4748 modules for the 4500 switching system unexpectedly drop traffic, considering them giants (any Ethernet packet that is greater than 1518 bytes is considered a giant). Affected modules include:
  - WS-X4748-UPOE+E
  - WS-X4748-RJ45V+E

  The problem is seen only on modules running Cisco IOS Release IOS-XE 03.02.n.SG. Certain revisions of the X4748 module display this behavior when running on IOS-XE version 03.02.n.SG. Not all X4748 modules will present this behavior, and it will not show up on newer versions of IOS-XE like 03.04.n.SG or 03.06.n.E.

  Workaround: Increasing the MTU on an affected interface to 1518 or higher will allow the traffic through. Upgrading to an IOS-XE version where this issue is not present will resolve the issue. CSCus15382

Resolved Caveats for Cisco IOS XE Release 3.2.9SG

This section lists the resolved caveats for Cisco IOS XE Release 3.2.9SG:

- The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:
  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation. Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml. CSCtd10712

- The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  Note Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven 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 2013 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_mar13.html CSCtg47129

- Configuring the **event Netflow exit-value** command for event4 causes a traceback

  Workaround: None - You cannot configure the event4 exit-value. CSCtl70569

- The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability. Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

  Note Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each 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 vulnerabilities in the March 2012 bundled publication.

  Individual publication links are in "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:
  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html. CSCts38429

- ES20 LC crash observed on router reload / LC OIR.

  Crash is observed in the following conditions -

  - router reload / LC OIR with images after RLS10.
  - traffic flows through the ES20 interface
  - mac-address-table limit CLI is configured.

Note Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each 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 vulnerabilities in the March 2012 bundled publication.
Individual publication links are in "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:
http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

Workaround: Remove mac-address-table limit. CSCtt28573

- The Cisco IOS Software implementation of the Network Address Translation (NAT) feature contains two vulnerabilities when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-nat

  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. See published Cisco Security Advisory. CSCue00996

- Minor or major temperature alarms are reported in the syslog along with the following DATACORRUPTION logs:

```
Aug  5 15:54:30.972 Buc:  DATACORRUPTION-SP-1-DATAINCONSISTENCY  copy error,  -PC=
0x414DEED4z
-Traceback= 4027C4F4 419551C0 414DEED4 414E5BC4 414E0CA0 414E0F00
Aug  5 15:54:30.972 Buc:  C6KENV-SP-4-MINORTEMPALARM  interface 10/0 outlet
temperature crossed threshold #1(=60C). It has exceeded normal operating temperature
range.
```

  The symptom is observed on ES+ series linecards of Cisco 7600 Series Routers.

  Workaround: None CSCui65914

- When you enter the **wr mem** command, the following error message is displayed:

```
private-config file open failed (File table overflow)
```

  This happens when you continuously reload the standby switch. The client, that is, the active side cannot reach the standby side, and while returning an error, the FD is not released and exhausts FDs. The maximum number of allowed FDs is 128. When this limit is reached, additional files cannot be opened.

  Workaround: Reload the switch. CSCug77784

- One or more interfaces on WS-X4748-RJ45V+E stop receiving traffic, making the interface unusable even after entering the **shutdown** and **no shutdown** interface configuration commands. The **show interface** privileged EXEC command indicates that the interface still sends data, but traffic is only unidirectional.

  Workarounds:

  - Reseat the line card (or hardware mod reset)
  - Reload the switch.

  Both are only temporary workarounds; the failure continues to resurface. CSCui36462

- A PoE device connected to an interface on module WS-X4748-UPOE+E will not power up. The interface will stay down or disconnected. entering the **shutdown** and **no shutdown** interface configuration commands has no effect.

  Any release prior to Cisco IOS Release 3.2.9SG, 3.4.4SG, and 3.6.0E (3.5.0E and 3.5.1E also have the issue.

  Workaround: Enter the **test cable-diagnostics tdr interface int** interface configuration command, to run TDR on the port. CSCui45222

- The Cisco Catalyst 4500 Series Switch crashes occasionally when multiple, simultaneous web authentication sessions affect the switch.

  Workaround: Avoid custom pages. CSCui71349

- TDR tests results for a port on a WS-X4748-UPOE+E linecard displays Unsupported in the Status field - which is incorrect. Sample output:

```
Switch # show cable-diagnostics tdr interface gigabitEthernet 1/1
Interface Speed  Local pair Cable length Remote channel Status
Gi1/1     0Mbps   1-2       6553 +/-1m    Unknown       Unsupported
                  3-6       6553 +/-1m    Unknown       Unsupported
                  4-5       6553 +/-1m    Unknown       Unsupported
                  7-8          0 m        Unknown       Unsupported
```

Workaround: Run TDR twice. CSCuj58332

- MAB does not trigger for devices if they are connected to a port before authentication is configured, provided the port is configured in authentication open mode.

  Workaround: Issue clear mac address dynamic to clear the MAC addresses on the switch and cause MAB to trigger when the MAC address is re-learned. CSCul32730

- The FFM process takes up progressively more memory and the free memory depletes by roughly the same amount - if the following conditions exist:
  - A consistent rapid flapping of mroutes.
  - Constant traffic toward a group on a VLAN where the SVI has PIM sparse mode configured, but an RP is not permitted for the group.

  Workarounds:
  - For flapping mroutes, track down the flapping mroute and prevent it.
  - For a missing RP scenario, either turn off PIM on the VLAN or allow the multicast group to associate with an RP. CSCul44174

- After upgrading to Cisco IOS Release 3.2.7SG and given more than 1024 active groups, both supervisor engines experience multicast packet loss and the number of S, Gs drops continuously.

  Workaround: None. CSCuo18934

- Upon one billion updates after booting, the switch crashes several times with the following log message:

  ```
  Apr  6 18:58:54.486: %IOSXE-2-PLATFORM: process ng_dumper: Process ffm: terminated
  abnormally.
  ```

  Workaround: Reboot the system at a minimally inconvenient time before 1 billion updates have occurred. CSCuo26294

- When an open-ring REP segment is configured with preemption, it fails to revert to a well-known topology after link state change between a pair of transit neighbors.

  Workaround: None. CSCuo51767

- Problem with adding new ports to a channel group. When you configure the **switchport private-vlan mapping trunk <vlan#1> <vlan#2>** command on a port and try to add that port to a channel group where the **switchport private-vlan mapping trunk** command is not configured, the following error message is displayed:

  ```
  Apr 23 00:36:33.772 JST: %EC-5-CANNOT_BUNDLE2: Gi6/1 is not compatible with Gi6/3 and
  will be suspended (mismatch on Secondary VLAN list on trunk)
  ```

  Workaround: None. CSCuo89407

- Software returns incorrect permanent license type (MIB value) from day 1. The license MIB value should be 4, but the software returns zero. The enum value cannot be changed because it leads to an ISSU breakage (a new TDL version is introduced).

  Workaround: None. The license MIB value for the permanent license type is 4 for all Cisco Catalyst 4000 series products. CSCuo90172

- Removing a VLAN Mapping statement causes all traffic to be consistently dropped for other VLAN mapping statements.

  Workarounds:
  - If you want to remove VLAN mapping on 12, but you need mapping on 13 to work, perform these steps:

a.Enter the **interface gigabitethernet 2/1** interface configuration command

b.Enter the **no switchport vlan mapping 12 dot1q-tunnel 200** interface configuration command

c.Enter the **no switchport vlan mapping 13 dot1q-tunnel 200** interface configuration command

d.Enter the **switchport vlan mapping 13 dot1q-tunnel 200** interface configuration command

– If you want to restore the original VLAN mapping statement, perform these steps

a.Enter the **interface gigabitethernet 2/1** interface configuration command

b.Enter the **no switchport vlan mapping 12 dot1q-tunnel 200** interface configuration command

c.Enter the **switchport vlan mapping 12 dot1q-tunnel 200** interface configuration command

– Enter the **shutdown** interface configuration command to shut down the port, remove configuration, and then enter the **no shutdown** interface configuration command. CSCum12826

- When you configure the **ip igmp mroute-proxy** interface configuration command and you reload the switch, the switch removes the command. The following example illustrates this problem:

```
interface Vlan14
ip address 10.1.1.1 255.255.255.252
ip pim sparse-mode
ip igmp mroute-proxy Vlan2137
end
48 Gigabit Ethernet interface
2 Ten Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.

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

Workaround: Reapply the configuration when the switch reboots. CSCum71764

Resolved Caveats for Cisco IOS XE Release 3.2.8SG

This section lists the resolved caveats for Cisco IOS XE Release 3.2.8SG:

- If you configure Open Authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new standby supervisor engine. The issue interrupts traffic only after the second switchover, because after the initial switchover the new standby supervisor engine possesses the wrong state, and the second switchover will start the port in the blocking state.

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

- If REP is configured on a dot1q trunk and the native VLAN is administratively set to a non-default value, REP packets are not sent on the native VLAN.

  Workaround: Retain the trunk native V LAN as 1. CSCud05521

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

  Workaround: Shorten the dACL name. CSCug78653

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

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

  CSCue62019

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

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

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

- If a device is authenticating while the RADIUS server goes down, the port connected to the device may enter the err-disabled state.

  Workaround: Configure RADIUS test and dead criteria.

  Example:

  ```
  radius-server dead-criteria time 10 tries 2
  radius-server host <ip> test username test key <key>
  radius-server deadtime 10
  ```

  CSCtn92693

- An SNMP walk of the LLDP MIB (OID 1.0.8802.1.1.2.1.5.4795) times out and produces a message similar to the following:

  ```
  Jun 19 10:48:51.835 UTC: %SYS-3-CPUHOG: Task is running for (2016)msecs, more than
  (2000)msecs (5/5),process = SNMP ENGINE.
  ```

  Workaround: Exclude the mib "lldpXMedMIB" with the **snmp-server view restrict lldpXMedMIB excluded** command. CSCuh88726

Open Caveats for Cisco IOS XE Release 3.2.7SG

This section lists the open caveats for Cisco IOS XE Release 3.2.7SG:

- When collecting data from the cpmCPUProcessHistoryTable, the data takes a long time to provide and the CPU utilization of the os_info_p process (OS Info provider) increases substantially. The time it takes to do a full walk of an almost fully populated table takes 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 attached to an SVI.

  This problem affects the Cisco Catalyst 4500 Series Supervisor 7E.

  Workaround: None. CSCth65129

- When either the RADIUS-server test feature or RADIUS-erver dead-criteria is configured and either RADIUS-server deadtime is not configured or is set to 0, 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 spanning tree is changed from PVST to Rapid PVST and you enter the **show spanning-tree vlan** command, the ports configured as promiscuous trunks are not listed as part of the spanning tree.

  Workaround: Enter **shut**, then **no shut** on the ports. CSCtn88228

- Unless you enter the **show mem detailed process** command on a Supervisor Engine 7-E switch, the parser chain is not displayed.

  Workaround: Enter the complete command string:

  ```
  show mem detailed process cli_agent
  ```

  CSCtj05663

- If you configure Open Authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new standby supervisor engine. The issue interrupts traffic only after the second switchover, because after the initial switchover the new standby supervisor engine possesses the wrong state, and the second switchover will start the port in the blocking state.

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

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

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

  CSCto27085

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

  Workaround: None. CSCto59368

- On Supervisor Engine 7-E, DBL might not funciton 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 occurs 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 capable of 2nd-port-TLV, 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 include advanced operators, including dscp/ipp/tos, log/log-input, fragments and/or tcp flag operators.

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

  Workaround: None. CSCtu37959

- On a redundant system consisting of supervisor engines 6-E and 7-E, when the system consumes 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 Supervisor Engine 6-E to match that of Supervisor Engine 7-E.

- Configuring an interface as uni-directional 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 bi-directional mode.

  Workaround: None. CSCtx95359

- If REP is configured on a dot1q trunk and the native VLAN is administratively set to a non-default value, REP packets are not sent on the native VLAN.

  Workaround: Retain the trunk native V LAN as 1. CSCud05521

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

  Workaround: Shorten the dACL name. CSCug78653

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

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

  CSCue62019

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

  – A fast stream of traffic matches the URL redirect ACL as IPDT clears an address.

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

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

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

- If a device is authenticating while the RADIUS server goes down, the port connected to the device may enter the err-disabled state.

  Workaround: Configure RADIUS test and dead criteria.

  Example:

  ```
  radius-server dead-criteria time 10 tries 2
  radius-server host <ip> test username test key <key>
  radius-server deadtime 10
  ```

  CSCtn92693

- An SNMP walk of the LLDP MIB (OID 1.0.8802.1.1.2.1.5.4795) times out and produces a message similar to the following:

  ```
  Jun 19 10:48:51.835 UTC: %SYS-3-CPUHOG: Task is running for (2016)msecs, more than
  (2000)msecs (5/5),process = SNMP ENGINE.
  ```

  Workaround: Exclude the mib "lldpXMedMIB" with the **snmp-server view restrict lldpXMedMIB excluded** command. CSCuh88726

Resolved Caveats for Cisco IOS XE Release 3.2.7SG

This section lists the resolved caveats for Cisco IOS XE Release 3.2.7SG:

- SFP modules GLC-SX-MMD and GLC-SH-LMD may not be recognized when used with the WS-X4448-GB-SFP linecard.

  Workarounds:

  - Use modules GLC-SX-MM and GLC-LH-SM instead.
  - Use a release other than IOS XE 3.2.0SG (or IOS 15.0(2)SG) through IOS XE 3.2.6SG (or IOS 15.0(2)SG6). CSCub52430

- On a Supervisor Engine 7-E running IOS Release XE 3.2.6SG and using PIM, a packet memory leak occurs when an "S,G entry" is created. When sufficient packets are leaked, IGMP packets are no longer processed and the switch must reload to restore service.

  Workaround: None. This issue does not occur in any other release, or in IOS Release XE 3.2.6SG when PIM is disabled. CSCue03401

Open Caveats for Cisco IOS XE Release 3.2.6SG

This section lists the open caveats for Cisco IOS XE Release 3.2.6SG:

- When collecting data from the cpmCPUProcessHistoryTable, the data takes a long time to provide and the CPU utilization of the os_info_p process (OS Info provider) increases substantially. The time it takes to do a full walk of an almost fully populated table takes 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 attached to an SVI.

  This problem affects the Cisco Catalyst 4500 Series Supervisor 7E.

  Workaround: None. CSCth65129

- When either the RADIUS-server test feature or RADIUS-erver dead-criteria is configured and either RADIUS-server deadtime is not configured or is set to 0, 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 spanning tree is changed from PVST to Rapid PVST and you enter the **show spanning-tree vlan** command, the ports configured as promiscuous trunks are not listed as part of the spanning tree.

  Workaround: Enter **shut**, then **no shut** on the ports. CSCtn88228

- Unless you enter the **show mem detailed process** command on a Supervisor Engine 7-E switch, the parser chain is not displayed.

  Workaround: Enter the complete command string:

  ```
  show mem detailed process cli_agent
  ```

  CSCtj05663

- If you configure Open Authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new standby supervisor engine. The issue interrupts traffic only after the second switchover, because after the initial switchover the new standby supervisor engine possesses the wrong state, and the second switchover will start the port in the blocking state.

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

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

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

  CSCto27085

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

  Workaround: None. CSCto59368

- On Supervisor Engine 7-E, DBL might not funciton 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 occurs 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 capable of 2nd-port-TLV, 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 include advanced operators, including dscp/ipp/tos, log/log-input, fragments and/or tcp flag operators.

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

  Workaround: None. CSCtu37959

- On a redundant system consisting of supervisor engines 6-E and 7-E, when the system consumes 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 Supervisor Engine 6-E to match that of Supervisor Engine 7-E.

- Configuring an interface as uni-directional 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 bi-directional mode.

  Workaround: None. CSCtx95359

- On a Supervisor Engine 7-E running IOS Release XE 3.2.6SG and using PIM, a packet memory leak occurs when an "S,G entry" is created. When sufficient packets are leaked, IGMP packets are no longer processed and the switch must reload to restore service.

  Workaround: None. This issue does not occur in any other release, or in IOS Release XE 3.2.6SG when PIM is disabled. CSCue03401

- If REP is configured on a dot1q trunk and the native VLAN is administratively set to a non-default value, REP packets are not sent on the native VLAN.

  Workaround: Retain the trunk native V LAN as 1. CSCud05521

- SFP modules GLC-SX-MMD and GLC-SH-LMD may not be recognized when used with the WS-X4448-GB-SFP linecard.

  Workarounds:

  - Use modules GLC-SX-MM and GLC-LH-SM instead.
  - Use a release other than IOS XE 3.2.0SG (or IOS 15.0(2)SG) through IOS XE 3.2.6SG (or IOS 15.0(2)SG6). CSCub52430

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

  Workaround: Shorten the dACL name. CSCug78653

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

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

  CSCue62019

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

  - A fast stream of traffic matches the URL redirect ACL as IPDT clears an address.
  - A traffic stream matches the URL redirect ACL and no URL redirect policy is installed for that IP address.

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

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

- If a device is authenticating while the RADIUS server goes down, the port connected to the device may enter the err-disabled state.

  Workaround: Configure RADIUS test and dead criteria.

Example:

```
radius-server dead-criteria time 10 tries 2
radius-server host <ip> test username test key <key>
radius-server deadtime 10
```

CSCtn92693

- An SNMP walk of the LLDP MIB (OID 1.0.8802.1.1.2.1.5.4795) times out and produces a message similar to the following:

```
Jun 19 10:48:51.835 UTC: %SYS-3-CPUHOG: Task is running for (2016)msecs, more than
(2000)msecs (5/5),process = SNMP ENGINE.
```

Workaround: Exclude the mib "lldpXMedMIB" with the **snmp-server view restrict lldpXMedMIB excluded** command. CSCuh88726

Resolved Caveats for Cisco IOS XE Release 3.2.6SG

This section lists the resolved caveats for Cisco IOS XE Release 3.2.6SG:

- A %SYS-2-NOBLOCK or %SYS-2-BLOCKHUNG message may appear on the switch when an interface with a QoS policy changes speed at the same time information about that interface is being collected (most commonly through a CLI like the **show policy-map ...** command). Although the QoS policy programming might fail for that interface, no operational impact is observed.

  Workaround: None. CSCtk52874

- In a square Layer 2 topology (of at least four switches) where the root bridge is outside of the square (a fifth switch), one link in the square that transitions its role from alternate to root will not send topology change notifications. A stale MAC address may exist in the table until age-out.

  Workaround: Reduce MAC aging time or modify Layer 2 topology so that the root is within the square. CSCtx86107

- A switch crashes after displaying the message

```
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9
```

  provided the following conditions apply:

  – A switchport is configured with the following:

    authentication event server dead action authorize

    authenticaton 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 the IAB-authorized port transitions to another state.

  Workaround: None. CSCtx61557

- The default SNMP engine ID is the same on Supervisor Engine 7-E switches running releases prior to IOS XE 3.2.6SG.

  Workaround: Configure an SNMP engine ID. CSCts87275

- IPSec frames less than 74 bytes are “dropped” on 4748 linecards and Supervisor Engine 7-E uplink ports. (IPsec is supported for management traffic only)

  Workaround: None. CSCub00709

Open Caveats for Cisco IOS XE Release 3.2.5SG

This section lists the open caveats for Cisco IOS XE Release 3.2.5SG:

- When collecting data from the cpmCPUProcessHistoryTable, the data takes a long time to provide and the CPU utilization of the os_info_p process (OS Info provider) increases substantially. The time it takes to do a full walk of an almost fully populated table takes 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 attached to an SVI.

  This problem affects the Cisco Catalyst 4500 Series Supervisor 7E.

  Workaround: None. CSCth65129

- When either the RADIUS-server test feature or RADIUS-erver dead-criteria is configured and either RADIUS-server deadtime is not configured or is set to 0, 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 spanning tree is changed from PVST to Rapid PVST and you enter the **show spanning-tree vlan** command, the ports configured as promiscuous trunks are not listed as part of the spanning tree.

  Workaround: Enter **shut**, then **no shut** on the ports. CSCtn88228

- Unless you enter the **show mem detailed process** command on a Supervisor Engine 7-E switch, the parser chain is not displayed.

  Workaround: Enter the complete command string:

  ```
  show mem detailed process cli_agent
  ```

  CSCtj05663

- If you configure Open Authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new standby supervisor engine. The issue interrupts traffic only after the second switchover, because after the initial switchover the new standby supervisor engine possesses the wrong state, and the second switchover will start the port in the blocking state.

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

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

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

  CSCto27085

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

  Workaround: None. CSCto59368

- On Supervisor Engine 7-E, DBL might not funciton 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 occurs 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 capable of 2nd-port-TLV, 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 include advanced operators, including dscp/ipp/tos, log/log-input, fragments and/or tcp flag operators.

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

  Workaround: None. CSCtu37959

- On a redundant system consisting of supervisor engines 6-E and 7-E, when the system consumes 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 Supervisor Engine 6-E to match that of Supervisor Engine 7-E.

- Configuring an interface as uni-directional 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 bi-directional mode.

  Workaround: None. CSCtx95359

- If REP is configured on a dot1q trunk and the native VLAN is administratively set to a non-default value, REP packets are not sent on the native VLAN.

  Workaround: Retain the trunk native V LAN as 1. CSCud05521

- SFP modules GLC-SX-MMD and GLC-SH-LMD may not be recognized when used with the WS-X4448-GB-SFP linecard.

  Workarounds:
  - Use modules GLC-SX-MM and GLC-LH-SM instead.
  - Use a release other than IOS XE 3.2.0SG (or IOS 15.0(2)SG) through IOS XE 3.2.6SG (or IOS 15.0(2)SG6). CSCub52430

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

  Workaround: Shorten the dACL name. CSCug78653

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

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

  CSCue62019

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

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

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

- If a device is authenticating while the RADIUS server goes down, the port connected to the device may enter the err-disabled state.

  Workaround: Configure RADIUS test and dead criteria.

  Example:

  ```
  radius-server dead-criteria time 10 tries 2
  radius-server host <ip> test username test key <key>
  radius-server deadtime 10
  ```

  CSCtn92693

- An SNMP walk of the LLDP MIB (OID 1.0.8802.1.1.2.1.5.4795) times out and produces a message similar to the following:

  ```
  Jun 19 10:48:51.835 UTC: %SYS-3-CPUHOG: Task is running for (2016)msecs, more than
  (2000)msecs (5/5),process = SNMP ENGINE.
  ```

  Workaround: Exclude the mib "lldpXMedMIB" with the **snmp-server view restrict lldpXMedMIB excluded** command. CSCuh88726

Resolved Caveats for Cisco IOS XE Release 3.2.5SG

This section lists the resolved caveats for Cisco IOS XE Release 3.2.5SG:

- On a switch running Cisco IOS Release 3.2.4SG or 3.3.0SG using 4648* or 4748* PoE linecards with connected devices that link flap frequently, a single port on a linecard fails to link up.

  Workaround: Enter **shut** then **no shut** the port to restore connectivity. CSCtz94862

- On a switch running Cisco IOS Release 3.2.4SG or 3.3.0SG using 4648* or 4748* linecards with PoE, a PoE device will not power up on a single port whereas it works on a different port on the same switch.

  Workarounds:

  - Connecting a non-PoE device
  - Enter **shut** then **no shut** on the port. CSCua63562

- If a switch is configured with the **aaa accounting send stop-record authentication failure** command, and MAB fails on the port and subsequent attempts are made to authorize the device after the restart timer expires, a high level of memory usage due to the "MAB Framework" process is observed.

  Workaround: Unconfigure the following from the switch: **aaa accounting send stop-record authentication failure**. CSCtj69212

Open Caveats for Cisco IOS XE Release 3.2.4SG

This section lists the open caveats for Cisco IOS XE Release 3.2.4SG:

- When collecting data from the cpmCPUProcessHistoryTable, the data takes a long time to provide and the CPU utilization of the os_info_p process (OS Info provider) increases substantially. The time it takes to do a full walk of an almost fully populated table takes 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 attached to an SVI.

  This problem affects the Cisco Catalyst 4500 Series Supervisor 7E.

  Workaround: None. CSCth65129

- When either the RADIUS-server test feature or RADIUS-erver dead-criteria is configured and either RADIUS-server deadtime is not configured or is set to 0, 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 spanning tree is changed from PVST to Rapid PVST and you enter the **show spanning-tree vlan** command, the ports configured as promiscuous trunks are not listed as part of the spanning tree.

  Workaround: Enter **shut**, then **no shut** on the ports. CSCtn88228

- Unless you enter the **show mem detailed process** command on a Supervisor Engine 7-E switch, the parser chain is not displayed.

  Workaround: Enter the complete command string:

  ```
  show mem detailed process cli_agent
  ```

  CSCtj05663

- If you configure Open Authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new standby supervisor engine. The issue interrupts traffic only after the second switchover, because after the initial switchover the new standby supervisor engine possesses the wrong state, and the second switchover will start the port in the blocking state.

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

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

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

  CSCto27085

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

  Workaround: None. CSCto59368

- On Supervisor Engine 7-E, DBL might not funciton 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 occurs 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 capable of 2nd-port-TLV, 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 include advanced operators, including dscp/ipp/tos, log/log-input, fragments and/or tcp flag operators.

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

  Workaround: None. CSCtu37959

- On a redundant system consisting of supervisor engines 6-E and 7-E, when the system consumes 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 Supervisor Engine 6-E to match that of Supervisor Engine 7-E.

- Configuring an interface as uni-directional 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 bi-directional mode.

  Workaround: None. CSCtx95359

- On a switch running Cisco IOS Release 3.2.4SG or 3.3.0SG using 4648* or 4748* PoE linecards with connected devices that link flap frequently, a single port on a linecard fails to link up.

  Workaround: Enter **shut** then **no shut** the port to restore connectivity. CSCtz94862

- On a switch running Cisco IOS Release 3.2.4SG or 3.3.0SG using 4648* or 4748* linecards with PoE, a PoE device will not power up on a single port whereas it works on a different port on the same switch.

  Workarounds:

  - Connecting a non-PoE device
  - Enter **shut** then **no shut** on the port. CSCua63562

- If a switch is configured with the **aaa accounting send stop-record authentication failure** command, and MAB fails on the port and subsequent attempts are made to authorize the device after the restart timer expires, a high level of memory usage due to the "MAB Framework" process is observed.

  Workaround: Unconfigure the following from the switch: **aaa accounting send stop-record authentication failure**. CSCtj69212

- If REP is configured on a dot1q trunk and the native VLAN is administratively set to a non-default value, REP packets are not sent on the native VLAN.

  Workaround: Retain the trunk native V LAN as 1. CSCud05521

- SFP modules GLC-SX-MMD and GLC-SH-LMD may not be recognized when used with the WS-X4448-GB-SFP linecard.

  Workarounds:

  - Use modules GLC-SX-MM and GLC-LH-SM instead.
  - Use a release other than IOS XE 3.2.0SG (or IOS 15.0(2)SG) through IOS XE 3.2.6SG (or IOS 15.0(2)SG6). CSCub52430
  -

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

  Workaround: Shorten the dACL name. CSCug78653

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

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

  CSCue62019

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

  - A fast stream of traffic matches the URL redirect ACL as IPDT clears an address.
  - A traffic stream matches the URL redirect ACL and no URL redirect policy is installed for that IP address.

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

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

- If a device is authenticating while the RADIUS server goes down, the port connected to the device may enter the err-disabled state.

  Workaround: Configure RADIUS test and dead criteria.

Example:

```
radius-server dead-criteria time 10 tries 2
radius-server host <ip> test username test key <key>
radius-server deadtime 10
```

CSCtn92693

- An SNMP walk of the LLDP MIB (OID 1.0.8802.1.1.2.1.5.4795) times out and produces a message similar to the following:

  ```
  Jun 19 10:48:51.835 UTC: %SYS-3-CPUHOG: Task is running for (2016)msecs, more than
  (2000)msecs (5/5),process = SNMP ENGINE.
  ```

  Workaround: Exclude the mib "lldpXMedMIB" with the **snmp-server view restrict lldpXMedMIB excluded** command. CSCuh88726

Resolved Caveats for Cisco IOS XE Release 3.2.4SG

This section lists the resolved caveats for Cisco IOS XE Release 3.2.4SG:

- If you use Supervisor Engine 7E or Supervisor Engine 7L-E and you enter either the **show redundancy** or commands beginning with the keyword **redundancy**, the following error displays:

  ```
  Failed to find pr_handlers by uri
  ```

  .**Workaround**: None. A reload is required to restore these commands. CSCtw95861

- When you execute the **show flow monitor** *monitor_name params* **top** *number* command simultaneously from different terminals to display the top flows, the supervisor engine might crash.

  Workaround: Avoid entering flexible netflow **show** commands from more than one terminal, when you want to display the top flows. CSCtw61872

- After a switch reestablishes a lost connection with AAA servers configured for broadcast accounting, the switch crashes.

  Workaround: Do not use the **broadcast** keyword in the aaa accounting configuration. CSCts56125

- A switch configured with 802.1X might shows considerable CPU usage by the 802.1X switch process and displays the following message:

  ```
  SYS-2-MALLOCFAIL messages, and - on redundant systems - begins logging EM-4-SENDFAILED
  messages,
  ```

  The occurs under the following conditions:

  - Multi-auth (or multi-host) and MAB dot1x are configured on a port.
  - A voice VLAN is not configured on the port.
  - The device authenticates through 802.1X.
  - The connected device sends no traffic, falls over to MAB, and then successfully authenticates through 802.1X.
  - A dynamic VLAN is assigned to the port following 802.1X authorization.

  Workarounds:

  - Enter **shut** then **no shut** on the port to halt the high CPU and log messages.
  - Enter the **switchport voice vlan** command on the port. CSCtw73754

- If PoE linecards are present and you enter either the **show power inline module** *x* or **show power inline module** *x* **detail** command, very rarely the supervisor engine might crash.

  Workaround: None. CSCtx25697

- After a few hours of operation, during which DHCP is enabled and sessions receive DHCP information from a RADIUS server, a Cisco ASR router running as an LNS box crashes with DHCP related errors.

  Workaround: None. CSCtj48387

- On a Supervisor Engine 7 running Cisco XE Release 3.2.2SG or 3.2.3SG, SNMP polling of CISCO-PROCESS-MIB data may cause high CPU and SNMP polling timeouts.

  Workaround: Use the sample below to restrict SNMP polling from retrieving 1.3.6.1.4.1.9.9.109:

  ```
  snmp-server view exampleview 1.3.6.1.4.1.9.9.109 exclude
  snmp-server community examplecommunity view exampleview RO
  ```

  CSCty18171

Open Caveats for Cisco IOS XE Release 3.2.3SG

This section lists the open caveats for Cisco IOS XE Release 3.2.3SG:

- When collecting data from the cpmCPUProcessHistoryTable, the data takes a long time to provide and the CPU utilization of the os_info_p process (OS Info provider) increases substantially. The time it takes to do a full walk of an almost fully populated table takes 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 attached to an SVI.

  This problem affects the Cisco Catalyst 4500 Series Supervisor 7E.

  Workaround: None. CSCth65129

- When either the RADIUS-server test feature or RADIUS-erver dead-criteria is configured and either RADIUS-server deadtime is not configured or is set to 0, 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 spanning tree is changed from PVST to Rapid PVST and you enter the **show spanning-tree vlan** command, the ports configured as promiscuous trunks are not listed as part of the spanning tree.

  Workaround: Enter **shut**, then **no shut** on the ports. CSCtn88228

- Unless you enter the **show mem detailed process** command on a Supervisor Engine 7-E switch, the parser chain is not displayed.

  Workaround: Enter the complete command string:

  ```
  show mem detailed process cli_agent
  ```

  CSCtj05663

- If you configure Open Authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new standby supervisor engine. The issue interrupts traffic only after the second switchover, because after the initial switchover the new standby supervisor engine possesses the wrong state, and the second switchover will start the port in the blocking state.

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

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

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

  CSCto27085

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

  Workaround: None. CSCto59368

- On Supervisor Engine 7-E, DBL might not funciton 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 occurs 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 capable of 2nd-port-TLV, 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 include advanced operators, including dscp/ipp/tos, log/log-input, fragments and/or tcp flag operators.

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

  Workaround: None. CSCtu37959

- On a redundant system consisting of supervisor engines 6-E and 7-E, when the system consumes 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 Supervisor Engine 6-E to match that of Supervisor Engine 7-E.

- If you use Supervisor Engine 7E or Supervisor Engine 7L-E and you enter either the **show redundancy** or commands beginning with the keyword **redundancy**, the following error displays:

  ```
  Failed to find pr_handlers by uri
  ```

  .**Workaround**: None. A reload is required to restore these commands. CSCtw95861

- When you execute the **show flow monitor** *monitor_name params* **top** *number* command simultaneously from different terminals to display the top flows, the supervisor engine might crash.

Workaround: Avoid entering fleible netflow **show** commands from more than one terminal, when you want to display the top flows. CSCtw61872

- After a switch reestablishes a lost connection with AAA servers configured for broadcast accounting, the switch crashes.

  Workaround: Do not use the **broadcast** keyword in the aaa accounting configuration. CSCts56125

- A switch configured with 802.1X might shows considerable CPU usage by the 802.1X switch process and displays the following message:

  ```
  SYS-2-MALLOCFAIL messages, and - on redundant systems - begins logging EM-4-SENDFAILED
  messages,
  ```

  The occurs under the following conditions:

  - Multi-auth (or multi-host) and MAB dot1x are configured on a port.
  - A voice VLAN is not configured on the port.
  - The device authenticates through 802.1X.
  - The connected device sends no traffic, falls over to MAB, and then successfully authenticates through 802.1X.
  - A dynamic VLAN is assigned to the port following 802.1X authorization.

  Workarounds:

  - Enter **shut** then **no shut** on the port to halt the high CPU and log messages.
  - Enter the **switchport voice vlan** command on the port. CSCtw73754

- If PoE linecards are present and you enter either the **show power inline module** *x* or **show power inline module** *x* **detail** command, very rarely the supervisor engine might crash.

  Workaround: None. CSCtx25697

- After a few hours of operation, during which DHCP is enabled and sessions receive DHCP information from a RADIUS server, a Cisco ASR router running as an LNS box crashes with DHCP related errors.

  Workaround: None. CSCtj48387

- On a Supervisor Engine 7 running Cisco XE Release 3.2.2SG or 3.2.3SG, SNMP polling of CISCO-PROCESS-MIB data may cause high CPU and SNMP polling timeouts.

  Workaround: Use the sample below to restrict SNMP polling from retrieving 1.3.6.1.4.1.9.9.109:

  ```
  snmp-server view exampleview 1.3.6.1.4.1.9.9.109 exclude
  snmp-server community examplecommunity view exampleview RO
  ```

  CSCty18171

- Configuring an interface as uni-directional 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 bi-directional mode.

  Workaround: None. CSCtx95359

- If a switch is configured with the **aaa accounting send stop-record authentication failure** command, and MAB fails on the port and subsequent attempts are made to authorize the device after the restart timer expires, a high level of memory usage due to the "MAB Framework" process is observed.

  Workaround: Unconfigure the following from the switch: **aaa accounting send stop-record authentication failure**. CSCtj69212

- If REP is configured on a dot1q trunk and the native VLAN is administratively set to a non-default value, REP packets are not sent on the native VLAN.

  Workaround: Retain the trunk native V LAN as 1. CSCud05521

- SFP modules GLC-SX-MMD and GLC-SH-LMD may not be recognized when used with the WS-X4448-GB-SFP linecard.

  Workarounds:

  - Use modules GLC-SX-MM and GLC-LH-SM instead.
  - Use a release other than IOS XE 3.2.0SG (or IOS 15.0(2)SG) through IOS XE 3.2.6SG (or IOS 15.0(2)SG6). CSCub52430
  -

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

  Workaround: Shorten the dACL name. CSCug78653

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

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

  CSCue62019

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

  - A fast stream of traffic matches the URL redirect ACL as IPDT clears an address.
  - A traffic stream matches the URL redirect ACL and no URL redirect policy is installed for that IP address.

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

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

- If a device is authenticating while the RADIUS server goes down, the port connected to the device may enter the err-disabled state.

  Workaround: Configure RADIUS test and dead criteria.

  Example:

  ```
  radius-server dead-criteria time 10 tries 2
  radius-server host <ip> test username test key <key>
  radius-server deadtime 10
  ```

  CSCtn92693

- An SNMP walk of the LLDP MIB (OID 1.0.8802.1.1.2.1.5.4795) times out and produces a message similar to the following:

```
Jun 19 10:48:51.835 UTC: %SYS-3-CPUHOG: Task is running for (2016)msecs, more than
(2000)msecs (5/5),process = SNMP ENGINE.
```

Workaround: Exclude the mib "lldpXMedMIB" with the **snmp-server view restrict lldpXMedMIB excluded** command. CSCuh88726

Resolved Caveats for Cisco IOS XE Release 3.2.3SG

This section lists the resolved caveats for Cisco IOS XE Release 3.2.3SG:

- If a Supervisor Engine 7E is running Cisco IOS Release 3.2.2SG and a considerable quantity of simultaneous ACL, QoS, or Layer 3 programming occurs (usually on switch bootup), ACL, QoS and Layer 3 changes fail to take effect from that point forward.

  Workaround: None. The supervisor engine must be reloaded or failed over. CSCtw93728

Open Caveats for Cisco IOS XE Release 3.2.2SG

This section lists the open caveats for Cisco IOS XE Release 3.2.3SG:

- When collecting data from the cpmCPUProcessHistoryTable, the data takes a long time to provide and the CPU utilization of the os_info_p process (OS Info provider) increases substantially. The time it takes to do a full walk of an almost fully populated table takes 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 attached to an SVI.

  This problem affects the Cisco Catalyst 4500 Series Supervisor 7E.

  Workaround: None. CSCth65129

- When either the RADIUS-server test feature or RADIUS-erver dead-criteria is configured and either RADIUS-server deadtime is not configured or is set to 0, 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 spanning tree is changed from PVST to Rapid PVST and you enter the **show spanning-tree vlan** command, the ports configured as promiscuous trunks are not listed as part of the spanning tree.

  Workaround: Enter **shut**, then **no shut** on the ports. CSCtn88228

- Unless you enter the **show mem detailed process** command on a Supervisor Engine 7-E switch, the parser chain is not displayed.

  Workaround: Enter the complete command string:

```
show mem detailed process cli_agent
```

  CSCtj05663

- If you configure Open Authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new standby supervisor engine. The issue interrupts traffic only after the second switchover, because after the initial switchover the new standby supervisor engine possesses the wrong state, and the second switchover will start the port in the blocking state.

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

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

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

  CSCto27085

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

  Workaround: None. CSCto59368

- On Supervisor Engine 7-E, DBL might not funciton 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 occurs 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 capable of 2nd-port-TLV, 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 include advanced operators, including dscp/ipp/tos, log/log-input, fragments and/or tcp flag operators.

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

  Workaround: None. CSCtu37959

- If a Supervisor Engine 7E is running Cisco IOS Release 3.2.2SG and a considerable quantity of simultaneous ACL, QoS, or Layer 3 programming occurs (usually on switch bootup), ACL, QoS and Layer 3 changes fail to take effect from that point forward.

  Workaround: None. The supervisor engine must be reloaded or failed over. CSCtw93728

- On a redundant system consisting of supervisor engines 6-E and 7-E, when the system consumes 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 Supervisor Engine 6-E to match that of Supervisor Engine 7-E.

- If you use Supervisor Engine 7E or Supervisor Engine 7L-E and you enter either the **show redundancy** or commands beginning with the keyword **redundancy**, the following error displays:

  ```
  Failed to find pr_handlers by uri
  ```

  .**Workaround**: None. A reload is required to restore these commands. CSCtw95861

- When you execute the **show flow monitor** *monitor_name params* **top** *number* command simultaneously from different terminals to display the top flows, the supervisor engine might crash.

  Workaround: Avoid entering flexible netflow **show** commands from more than one terminal, when you want to display the top flows. CSCtw61872

- After a switch reestablishes a lost connection with AAA servers configured for broadcast accounting, the switch crashes.

  Workaround: Do not use the **broadcast** keyword in the aaa accounting configuration. CSCts56125

- A switch configured with 802.1X might shows considerable CPU usage by the 802.1X switch process and displays the following message:

  ```
  SYS-2-MALLOCFAIL messages, and - on redundant systems - begins logging EM-4-SENDFAILED
  messages,
  ```

  The occurs under the following conditions:

  - Multi-auth (or multi-host) and MAB dot1x are configured on a port.
  - A voice VLAN is not configured on the port.
  - The device authenticates through 802.1X.
  - The connected device sends no traffic, falls over to MAB, and then successfully authenticates through 802.1X.
  - A dynamic VLAN is assigned to the port following 802.1X authorization.

  Workarounds:

  - Enter **shut** then **no shut** on the port to halt the high CPU and log messages.
  - Enter the **switchport voice vlan** command on the port. CSCtw73754

- If PoE linecards are present and you enter either the **show power inline module** *x* or **show power inline module** *x* **detail** command, very rarely the supervisor engine might crash.

  Workaround: None. CSCtx25697

- After a few hours of operation, during which DHCP is enabled and sessions receive DHCP information from a RADIUS server, a Cisco ASR router running as an LNS box crashes with DHCP related errors.

  Workaround: None. CSCtj48387

- On a Supervisor Engine 7 running Cisco XE Release 3.2.2SG or 3.2.3SG, SNMP polling of CISCO-PROCESS-MIB data may cause high CPU and SNMP polling timeouts.

  Workaround: Use the sample below to restrict SNMP polling from retrieving 1.3.6.1.4.1.9.9.109:

  ```
  snmp-server view exampleview 1.3.6.1.4.1.9.9.109 exclude
  snmp-server community examplecommunity view exampleview RO
  ```

  CSCty18171

- Configuring an interface as uni-directional 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 bi-directional mode.

  Workaround: None. CSCtx95359

- If a switch is configured with the **aaa accounting send stop-record authentication failure** command, and MAB fails on the port and subsequent attempts are made to authorize the device after the restart timer expires, a high level of memory usage due to the "MAB Framework" process is observed.

  Workaround: Unconfigure the following from the switch: **aaa accounting send stop-record authentication failure**. CSCtj69212

- If REP is configured on a dot1q trunk and the native VLAN is administratively set to a non-default value, REP packets are not sent on the native VLAN.

  Workaround: Retain the trunk native V LAN as 1. CSCud05521

- SFP modules GLC-SX-MMD and GLC-SH-LMD may not be recognized when used with the WS-X4448-GB-SFP linecard.

  Workarounds:

  - Use modules GLC-SX-MM and GLC-LH-SM instead.
  - Use a release other than IOS XE 3.2.0SG (or IOS 15.0(2)SG) through IOS XE 3.2.6SG (or IOS 15.0(2)SG6). CSCub52430
  -

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

  Workaround: Shorten the dACL name. CSCug78653

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

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

  CSCue62019

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

  - A fast stream of traffic matches the URL redirect ACL as IPDT clears an address.
  - A traffic stream matches the URL redirect ACL and no URL redirect policy is installed for that IP address.

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

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

- If a device is authenticating while the RADIUS server goes down, the port connected to the device may enter the err-disabled state.

  Workaround: Configure RADIUS test and dead criteria.

Example:

```
radius-server dead-criteria time 10 tries 2
radius-server host <ip> test username test key <key>
radius-server deadtime 10
```

CSCtn92693

- An SNMP walk of the LLDP MIB (OID 1.0.8802.1.1.2.1.5.4795) times out and produces a message similar to the following:

```
Jun 19 10:48:51.835 UTC: %SYS-3-CPUHOG: Task is running for (2016)msecs, more than
(2000)msecs (5/5),process = SNMP ENGINE.
```

Workaround: Exclude the mib "lldpXMedMIB" with the **snmp-server view restrict lldpXMedMIB excluded** command. CSCuh88726

Resolved Caveats for Cisco IOS XE Release 3.2.2SG

This section lists the resolved caveats for Cisco IOS XE Release 3.2.2SG:

- If Flex link load balancing is configured on a PVLAN flex link pair and some VLANs prefer the backup interface in the pair, entering **shut** and then **no shut** on the backup flex link interface causes high cpu from SA miss events. This happens because dynamic mac address learning is broken.

  The primary flex link interface comes up correctly.

  Workaround: Configure static MAC address for the MAC address that must be learned dynamically on the backup flex link interface. CSCtr40070

- After booting a switch with Supervisor Engine 7-E, you observe two versions of incorrect up time when using **show version** or **show redundancy**:

  Scenario #1: Display 136 years, 10 weeks, 6 hours, 26 minutes

```
Current Processor Information :
-------------------------------

Active Location = slot 5
        Current Software state = ACTIVE
       Uptime in current state = 136 years, 10 weeks, 6 hours, 26 minutes
                 Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3
Switch Software (cat4500e-UNIVERSALK9-M), Version 03.01.01.SG RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 14-Dec-10 22:12 by prod
               BOOT = bootflash:cat4500e-universalk9.SPA.03.01.01.SG.150-1.XO1.bin,1;
        Configuration register = 0x2102
```

  Scenario #2: Display “0 minute” after being up for a few days

```
Current Processor Information :
-------------------------------
               Active Location = slot 6
        Current Software state = ACTIVE
       Uptime in current state = 0 minute
                 Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3
Switch Software (cat4500e-UNIVERSALK9-M), Version 03.01.01.SG RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 14-Dec-10 22:12 by prod
               BOOT = bootflash:cat4500e-universalk9.SPA.03.01.01.SG.150-1.XO1.bin,1;
        Configuration register = 0x2102
```

Workaround: None. CSCtr54218

- When configuring, removing, and reapplying IP SLA configuration (reapply without the history filter) and querying the rttmonhistory tree, a Catalyst4 948-10GE switch will fail.

  Workaround: None. CSCtr52740

- Configuring and copying a TCL policy may cause a Catalyst 4500 series switch to hang.

  Workaround: None. CSCto72927

- Layer 2 multicast is not switched egress with a port-channel interface after a member link or port-channel flaps.

  Workaround:

  1. Delete, then add the affected VLAN with **no vlan** *vlan_ID*, then **lan** *vlan_ID.*

  2. Flap the impacted port-channel with **shutdown** then **no shutdown**. CSCtr17251

- When a switch is configured for MAC Authentication Bypass (MAB) EAP and the AAA server requests EAP-TLS (as the EAP method) first, MAB fails.

  Workarounds:

  - Configure the switch port for *mab* rather than *mab eap.*
  - Configure the AAA server to propose EAP-MD5 first rather than EAP-TLS for MAB EAP requests. CSCti78674

- One or more line cards (WS-X46xx and WS-X47xx series) stop responding to interface changes when near-simultaneous link events (if timed correctly) occur on the same linecard.

  Only line cards in the WS-X46xx series and the WS-X47xx series are affected. Interfaces that are already linked-up are not affected.

  Workaround: Eliminate link flap. If the problem exists, do one of the following:

  - Reload the linecard module with the **hw-module module** *n* **reset** command.
  - For dual supervisor engines, perform a switchover. CSCts67025

- Frequent link flap can trigger a failure that causes control plane latency until the switch is reloaded. After the issue is triggered, normal traffic is forwarded without drops, but pings to or from the switch drop, and new connections to linecards come up slowly or not at all. The following error messages appear:

  ```
  C4K_WATCHDOG-3-CHILDFAILURE:
  C4K_LINECARD-3-INTERRUPTDELAYED:
  C4K_LINECARD-3-INTERRUPTCOMPLETED:
  ```

  Workaround: Eliminate link flap.

  Provide temporary remediation with a forced supervisor engine switchover. CSCtt06131

- Occasionally, when an interface with a QoS policy changes speed or when a QoS policy is being programmed on an interface, a Supervisor Engine 7 might unexpectedly encounter an FFM crash.

  Workaround: None. CSCtn81726

- Rarely, an FFM crash may occur when control plane queues are slow to empty.

  Workaround: None. CSCtr07852

- A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

Note The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each 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 vulnerabilities in the March 2012 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_mar12.html

CSCtr28857

Open Caveats for Cisco IOS XE Release 3.2.1SG

This section lists the open caveats for Cisco IOS XE Release 3.2.1SG:

- When collecting data from the cpmCPUProcessHistoryTable, the data takes a long time to provide and the CPU utilization of the os_info_p process (OS Info provider) increases substantially. The time it takes to do a full walk of an almost fully populated table takes 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 attached to an SVI.

  This problem affects the Cisco Catalyst 4500 Series Supervisor 7E.

  Workaround: None. CSCth65129

- When either the RADIUS-server test feature or RADIUS-erver dead-criteria is configured and either RADIUS-server deadtime is not configured or is set to 0, 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 spanning tree is changed from PVST to Rapid PVST and you enter the **show spanning-tree vlan** command, the ports configured as promiscuous trunks are not listed as part of the spanning tree.

  Workaround: Enter **shut**, then **no shut** on the ports. CSCtn88228

- Unless you enter the **show mem detailed process** command on a Supervisor Engine 7-E switch, the parser chain is not displayed.

Workaround: Enter the complete command string:

```
show mem detailed process cli_agent
```

CSCtj05663

- If you configure Open Authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new standby supervisor engine. The issue interrupts traffic only after the second switchover, because after the initial switchover the new standby supervisor engine possesses the wrong state, and the second switchover will start the port in the blocking state.

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

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

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

  CSCto27085

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

  Workaround: None. CSCto59368

- On Supervisor Engine 7-E, DBL might not funciton 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 occurs 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 capable of 2nd-port-TLV, 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 Flex link load balancing is configured on a PVLAN flex link pair and some VLANs prefer the backup interface in the pair, entering **shut** and then **no shut** on the backup flex link interface causes high cpu from SA miss events. This happens because dynamic mac address learning is broken.

  The primary flex link interface comes up correctly.

  Workaround: Configure static MAC address for the MAC address that must be learned dynamically on the backup flex link interface. CSCtr40070

- After booting a switch with Supervisor Engine 7-E, you observe two versions of incorrect up time when using **show version** or **show redundancy**:

  Scenario #1: Display 136 years, 10 weeks, 6 hours, 26 minutes

```
Current Processor Information :
-------------------------------

Active Location = slot 5
        Current Software state = ACTIVE
       Uptime in current state = 136 years, 10 weeks, 6 hours, 26 minutes
                 Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3
Switch Software (cat4500e-UNIVERSALK9-M), Version 03.01.01.SG RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 14-Dec-10 22:12 by prod
               BOOT = bootflash:cat4500e-universalk9.SPA.03.01.01.SG.150-1.XO1.bin,1;
        Configuration register = 0x2102
```

Scenario #2: Display “0 minute” after being up for a few days

```
Current Processor Information :
-------------------------------
               Active Location = slot 6
        Current Software state = ACTIVE
       Uptime in current state = 0 minute
                 Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3
Switch Software (cat4500e-UNIVERSALK9-M), Version 03.01.01.SG RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 14-Dec-10 22:12 by prod
               BOOT = bootflash:cat4500e-universalk9.SPA.03.01.01.SG.150-1.XO1.bin,1;
        Configuration register = 0x2102
```

Workaround: None. CSCtr54218

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

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

  Workaround: None. CSCtu37959

- When a switch is configured for MAC Authentication Bypass (MAB) EAP and the AAA server requests EAP-TLS (as the EAP method) first, MAB fails.

  Workarounds:

  – Configure the switch port for *mab* rather than *mab eap.*

  – Configure the AAA server to propose EAP-MD5 first rather than EAP-TLS for MAB EAP requests. CSCti78674

- When configuring, removing, and reapplying IP SLA configuration (reapply without the history filter) and querying the rttmonhistory tree, a Catalyst4 948-10GE switch will fail.

  Workaround: None. CSCtr52740

- Layer 2 multicast is not switched egress with a port-channel interface after a member link or port-channel flaps.

  Workaround:

  1. Delete, then add the affected VLAN with **no vlan** *vlan_ID*, then **lan** *vlan_ID.*

  2. Flap the impacted port-channel with **shutdown**, then **no shutdown**. CSCtr17251

- Configuring and copying a TCL policy may cause a Catalyst 4500 series switch to hang.

  Workaround: None. CSCto72927

- One or more line cards (WS-X46xx and WS-X47xx series) stop responding to interface changes when near-simultaneous link events (if timed correctly) occur on the same linecard.

  Only line cards in the WS-X46xx series and the WS-X47xx series are affected. Interfaces that are already linked-up are not affected.

Workaround: Eliminate link flap. If the problem exists, do one of the following:

- Reload the linecard module with the **hw-module module** *n* **reset** command.
- For dual supervisor engines, perform a switchover. CSCts67025

- Frequent link flap can trigger a failure that causes control plane latency until the switch is reloaded. After the issue is triggered, normal traffic is forwarded without drops, but pings to or from the switch drop, and new connections to linecards come up slowly or not at all. The following error messages appear:

```
C4K_WATCHDOG-3-CHILDFAILURE:
C4K_LINECARD-3-INTERRUPTDELAYED:
C4K_LINECARD-3-INTERRUPTCOMPLETED:
```

Workaround: Eliminate link flap.

Provide temporary remediation with a forced supervisor engine switchover. CSCtt06131

- Occasionally, when an interface with a QoS policy changes speed or when a QoS policy is being programmed on an interface, a Supervisor Engine 7 might unexpectedly encounter an FFM crash.

Workaround: None. CSCtn81726

- A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

Note The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each 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 vulnerabilities in the March 2012 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_mar12.html

CSCtr28857

- Rarely, an FFM crash may occur when control plane queues are slow to empty.

Workaround: None. CSCtr07852

- If a Supervisor Engine 7E is running Cisco IOS Release 3.2.2SG and a considerable quantity of simultaneous ACL, QoS, or Layer 3 programming occurs (usually on switch bootup), ACL, QoS and Layer 3 changes fail to take effect from that point forward.

Workaround: None. The supervisor engine must be reloaded or failed over. CSCtw93728

- On a redundant system consisting of supervisor engines 6-E and 7-E, when the system consumes 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 Supervisor Engine 6-E to match that of Supervisor Engine 7-E.

- If you use Supervisor Engine 7E or Supervisor Engine 7L-E and you enter either the **show redundancy** or commands beginning with the keyword **redundancy**, the following error displays:

  ```
  Failed to find pr_handlers by uri
  ```

  .**Workaround**: None. A reload is required to restore these commands. CSCtw95861

- When you execute the **show flow monitor** *monitor_name params* **top** *number* command simultaneously from different terminals to display the top flows, the supervisor engine might crash.

  Workaround: Avoid entering flexible netflow **show** commands from more than one terminal, when you want to display the top flows. CSCtw61872

- After a switch reestablishes a lost connection with AAA servers configured for broadcast accounting, the switch crashes.

  Workaround: Do not use the **broadcast** keyword in the aaa accounting configuration. CSCts56125

- A switch configured with 802.1X might shows considerable CPU usage by the 802.1X switch process and displays the following message:

  ```
  SYS-2-MALLOCFAIL messages, and - on redundant systems - begins logging EM-4-SENDFAILED
  messages,
  ```

  The occurs under the following conditions:

  - Multi-auth (or multi-host) and MAB dot1x are configured on a port.
  - A voice VLAN is not configured on the port.
  - The device authenticates through 802.1X.
  - The connected device sends no traffic, falls over to MAB, and then successfully authenticates through 802.1X.
  - A dynamic VLAN is assigned to the port following 802.1X authorization.

  Workarounds:

  - Enter **shut** then **no shut** on the port to halt the high CPU and log messages.
  - Enter the **switchport voice vlan** command on the port. CSCtw73754

- If PoE linecards are present and you enter either the **show power inline module** *x* or **show power inline module** *x* **detail** command, very rarely the supervisor engine might crash.

  Workaround: None. CSCtx25697

- After a few hours of operation, during which DHCP is enabled and sessions receive DHCP information from a RADIUS server, a Cisco ASR router running as an LNS box crashes with DHCP related errors.

  Workaround: None. CSCtj48387

- Configuring an interface as uni-directional 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 bi-directional mode.

  Workaround: None. CSCtx95359

- If a switch is configured with the **aaa accounting send stop-record authentication failure** command, and MAB fails on the port and subsequent attempts are made to authorize the device after the restart timer expires, a high level of memory usage due to the "MAB Framework" process is observed.

  Workaround: Unconfigure the following from the switch: **aaa accounting send stop-record authentication failure**. CSCtj69212

- If REP is configured on a dot1q trunk and the native VLAN is administratively set to a non-default value, REP packets are not sent on the native VLAN.

  Workaround: Retain the trunk native V LAN as 1. CSCud05521

- SFP modules GLC-SX-MMD and GLC-SH-LMD may not be recognized when used with the WS-X4448-GB-SFP linecard.

  Workarounds:

  - Use modules GLC-SX-MM and GLC-LH-SM instead.
  - Use a release other than IOS XE 3.2.0SG (or IOS 15.0(2)SG) through IOS XE 3.2.6SG (or IOS 15.0(2)SG6). CSCub52430

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

  Workaround: Shorten the dACL name. CSCug78653

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

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

  CSCue62019

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

  - A fast stream of traffic matches the URL redirect ACL as IPDT clears an address.
  - A traffic stream matches the URL redirect ACL and no URL redirect policy is installed for that IP address.

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

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

- If a device is authenticating while the RADIUS server goes down, the port connected to the device may enter the err-disabled state.

  Workaround: Configure RADIUS test and dead criteria.

  Example:

  ```
  radius-server dead-criteria time 10 tries 2
  radius-server host <ip> test username test key <key>
  radius-server deadtime 10
  ```

  CSCtn92693

- An SNMP walk of the LLDP MIB (OID 1.0.8802.1.1.2.1.5.4795) times out and produces a message similar to the following:

```
Jun 19 10:48:51.835 UTC: %SYS-3-CPUHOG: Task is running for (2016)msecs, more than
(2000)msecs (5/5),process = SNMP ENGINE.
```

  Workaround: Exclude the mib "lldpXMedMIB" with the **snmp-server view restrict lldpXMedMIB excluded** command. CSCuh88726

Resolved Caveats for Cisco IOS XE Release 3.2.1SG

This section lists the resolved caveats for Cisco IOS XE Release 3.2.1SG:

- When you configure EnergyWise power control on PoE ports with a time-based execution schedule, time entry executes without adjusting for daylight savings time.

  Workaround: Manually re-enter all entries with new time settings.

  CSCsy27389

- Under Cisco IOS Release 15.0.1.XO, Control Plane Policing is missing class system-cgmp-cpp. When adding this class manually and then attaching a policer to this class, the policer matches on any IP packet.

  Workaround: Do not use or remove class system-cgmp-cpp. CSCtn46868

- After a session falls back to Web Authentication, and no port ACL or fallback ACL is configured, Auth_Default_ACL is programmed infrequently.

  Workaround: Configure a port ACL on the interface. CSCtl89389

- When re-connecting to a switch using device tracking, a Windows Vista, 2008, or 2007 device registers a duplicate address message. A Windows Vista, 2008, or 2007 client probes for a tentative IP address while the switch probes for device status. This issue is usually triggered by disconnecting or reconnecting.

  Workaround: Disable gratuitous ARPs on the Windows device. CSCtn27420

- If you create a new IPv6 ACL, delete a permit ACE, and then add back the permit ACE, the **sh run | b ipv6 access-list** command displays unexpected commands on the IPv6 access-list configuration.

```
sh run | b ipv6 access-list
ipv6 access-list ipv6acl
 permit icmp any FF01::/16
 permit icmp any FF02::/16
 sequence 40 permit icmp any FE80::/10
sequence 40 (appears in front of entry)
```

  In the output above, **sequence 40** is the unexpected command that appears in front of the entry.

  Workaround: Delete the access-list and reconfigure all entries, rather than deleting or reconfiguring the access-list. CSCtn83348

- A switch configured for **epm open directive** in multi-auth configuration fails when authentication sessions are cleared.

  Workaround: Do not configure open directive on the switch.

  CSCto48824

- A switch fails when you change the maximum login attempts value for a webauthentication session.

  Workaround: Modify max login attempts when webauth is not active. CSCtn17953

- During an SSO/ISSU operation, if an EEE linecard is OIR'd, removed or replaced, and the Ethernet Energy Efficient feature is configured on a given port, the configuration cannot be saved.

  Workaround: Deconfigure EEE before running SSO/ISSU or relocating an EE linecard; or reconfigure EEE again after the upgrade or linecard reinsertion.

  CSCto97743

- The power reported as delivered to a UPOE (greater than 30 watts) client may drop suddenly when a supervisor engine switchover occurs. The device still functions properly, provided power inline police is not enabled on the device's port.

  Workaround: Do not enable power inline police on ports delivering more than 30 watts in a redundant system. CSCtq32785

- A Supervisor Engine 7-E might fail when the output queuing policy is removed and readded through some range of interfaces that undergoes speed change or negotiation and the impacted interface has an attached queuing policy.

  Workaround: None. CSCtq57827

- On a Supervisor Engine 7-E, if an output service policy is applied on a port and that port is connected to a PC or other client device, some traffic appears to be dropped in the egress direction after boot up because of misprogrammed port TxQ.

  Workaround:Remove and readd the outbound service policy. CSCtq40350

- If you use IGMP reports with groups like 226.0.0.2, 225.0.0.2, or 225.128.0.2, HSRP hello packets drop and HSRP peers are down. This happens because HSRP hello packets are sent to MAC address 224.0.0.2, which overlaps with the IGMP group addresses just mentioed.

  Workaround: None. Use a different IGMP group address. CSCtq15982

- The list of VLANs defined by the **vlan-range** command used for configuring per-VLAN QoS is too long, causing the system to reject the command and display the following log:

  ```
  Command rejected: Bad VLAN list - character #"X" (EOL) delimits a VLAN number ("Y")
  end of range not larger than the start of range ("Z").
  ```

  Workaround: None CSCtr49819

- Switches using ESM logging filter TCL script will fail after some time.

  Workaround: Remove the logging filter. CSCto76709

- A Supervisor Engine 7-E will fail when the following applies when an ACL used by the class-map is modified to match new traffic and a control plane policy is currently attache.

  Workaround: Configure new class-maps and a policy-map. Replace the control plane policy with the new policy. CSCto45530

- A host IP is not inserted into a URL redirect ACL unless the host IP is already in the device tracking table (DHCP snooping or IPDT).

  Workaround: None. CSCtn63638

- A host IP is not inserted into a URL redirect ACL unless the host IP is already in the device tracking table (DHCP snooping or IPDT).

  Workaround: None. CSCtn63638

- DACLs, filter-ID, and proxy ACLs do not function correctly.

  Workaround: None. CSCto79232

- DACLs, filter-ID, and proxy ACLs do not function correctly.

  Workaround: None. CSCto79232

Open Caveats for Cisco IOS XE Release 3.2.0SG

This section lists the open caveats for Cisco IOS XE Release 3.2.0SG:

- When you configure EnergyWise power control on PoE ports with a time-based execution schedule, time entry executes without adjusting for daylight savings time.

  Workaround: Manually re-enter all entries with new time settings.

  CSCsy27389

- When collecting data from the cpmCPUProcessHistoryTable, the data takes a long time to provide and the CPU utilization of the os_info_p process (OS Info provider) increases substantially. The time it takes to do a full walk of an almost fully populated table takes 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 attached to an SVI.

  This problem affects the Cisco Catalyst 4500 Series Supervisor 7E.

  Workaround: None. CSCth65129

- Under Cisco IOS Release 15.0.1.XO, Control Plane Policing is missing class system-cgmp-cpp. When adding this class manually and then attaching a policer to this class, the policer matches on any IP packet.

  Workaround: Do not use or remove class system-cgmp-cpp. CSCtn46868

- Supervisor Engine 7-E running Cisco IOS XE 3.1.1(SG) crashes with FFM traceback when applying a qos policy to all the interfaces of a WS-X4748-RJ45V+E module with the **interface range** command.

  Workaround: None. CSCtn81726

- When either the RADIUS-server test feature or RADIUS-erver dead-criteria is configured and either RADIUS-server deadtime is not configured or is set to 0, 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

- After a session falls back to Web Authentication, and no port ACL or fallback ACL is configured, Auth_Default_ACL is programmed infrequently.

  Workaround: Configure a port ACL on the interface. CSCtl89389

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

  Workaround: Enter **shut**, then **no shut** on the ports. CSCtn88228

- Unless you enter the **show mem detailed process** command on a Supervisor Engine 7-E switch, the parser chain is not displayed.

  Workaround: Enter the complete command string:

  ```
  show mem detailed process cli_agent
  ```

  CSCtj05663

- When re-connecting to a switch using device tracking, a Windows Vista, 2008, or 2007 device registers a duplicate address message. A Windows Vista, 2008, or 2007 client probes for a tentative IP address while the switch probes for device status. This issue is usually triggered by disconnecting or reconnecting.

  Workaround: Disable gratuitous ARPs on the Windows device. CSCtn27420

- If you create a new IPv6 ACL, delete a permit ACE, and then add back the permit ACE, the **sh run | b ipv6 access-list** command displays unexpected commands on the IPv6 access-list configuration.

  ```
  sh run | b ipv6 access-list
  ipv6 access-list ipv6acl
   permit icmp any FF01::/16
   permit icmp any FF02::/16
   sequence 40 permit icmp any FE80::/10
  sequence 40 (appears in front of entry)
  ```

  In the output above, **sequence 40** is the unexpected command that appears in front of the entry.

  Workaround: Delete the access-list and reconfigure all entries, rather than deleting or reconfiguring the access-list. CSCtn83348

- If you configure Open Authentication and perform SSO, the spanning tree state and MAC address are not synchronized to the new standby supervisor engine. The issue interrupts traffic only after the second switchover, because after the initial switchover the new standby supervisor engine possesses the wrong state, and the second switchover will start the port in the blocking state.

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

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

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

  CSCto27085

- A switch configured for **epm open directive** in multi-auth configuration fails when authentication sessions are cleared.

  Workaround: Do not configure open directive on the switch.

  CSCto48824

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

  Workaround: None. CSCto59368

- On Supervisor Engine 7-E, DBL might not funciton 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 occurs during the upgrade process.

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

CSCto51562

- A switch fails when you change the maximum login attempts value for a webauthentication session.

  Workaround: Modify max login attempts when webauth is not active. CSCtn17953

- A device in a Guest VLAN that is connected behind a phone capable of 2nd-port-TLV, 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

- A host IP is not inserted into a URL redirect ACL unless the host IP is already in the device tracking table (DHCP snooping or IPDT).

  Workaround: None. CSCtn63638

- DACLs, filter-ID, and proxy ACLs do not function correctly.

  Workaround: None. CSCto79232

- If Filter ID or fallback ACLs are currently applied to a port, and you modify them, they will not be programmed correctly in hardware.

  Workaround: Modify filter ID or fallback ACLs only when they are not in use. CSCto79274

- During an SSO/ISSU operation, if an EEE linecard is OIR'd, removed or replaced, and the Ethernet Energy Efficient feature is configured on a given port, the configuration cannot be saved.

  Workaround: Deconfigure EEE before running SSO/ISSU or relocating an EE linecard; or reconfigure EEE again after the upgrade or linecard reinsertion.

  CSCto97743

- The power reported as delivered to a UPOE (greater than 30 watts) client may drop suddenly when a supervisor engine switchover occurs. The device still functions properly, provided power inline police is not enabled on the device's port.

  Workaround: Do not enable power inline police on ports delivering more than 30 watts in a redundant system. CSCtq32785

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

  Workaround: None. CSCtu37959

- When configuring, removing, and reapplying IP SLA configuration (reapply without the history filter) and querying the rttmonhistory tree, a Catalyst4 948-10GE switch will fail.

  Workaround: None. CSCtr52740

- Layer 2 multicast is not switched egress with a port-channel interface after a member link or port-channel flaps.

  Workaround:

  1. Delete, then add the affected VLAN with **no vlan** *vlan_ID*, then **lan** *vlan_ID*.

  2. Flap the impacted port-channel with **shutdown**, then **no shutdown**. CSCtr17251

- Configuring and copying a TCL policy may cause a Catalyst 4500 series switch to hang.

  Workaround: None. CSCto72927

- If Flex link load balancing is configured on a PVLAN flex link pair and some VLANs prefer the backup interface in the pair, entering **shut** and then **no shut** on the backup flex link interface causes high cpu from SA miss events. This happens because dynamic mac address learning is broken.

The primary flex link interface comes up correctly.

Workaround: Configure static MAC address for the MAC address that must be learned dynamically on the backup flex link interface. CSCtr40070

- When a switch is configured for MAC Authentication Bypass (MAB) EAP and the AAA server requests EAP-TLS (as the EAP method) first, MAB fails.

  Workarounds:

  - Configure the switch port for *mab* rather than *mab eap.*
  - Configure the AAA server to propose EAP-MD5 first rather than EAP-TLS for MAB EAP requests. CSCti78674

- One or more line cards (WS-X46xx and WS-X47xx series) stop responding to interface changes when near-simultaneous link events (if timed correctly) occur on the same linecard.

  Only line cards in the WS-X46xx series and the WS-X47xx series are affected. Interfaces that are already linked-up are not affected.

  Workaround: Eliminate link flap. If the problem exists, do one of the following:

  - Reload the linecard module with the **hw-module module** *n* **reset** command.
  - For dual supervisor engines, perform a switchover. CSCts67025

- Frequent link flap can trigger a failure that causes control plane latency until the switch is reloaded. After the issue is triggered, normal traffic is forwarded without drops, but pings to or from the switch drop, and new connections to linecards come up slowly or not at all. The following error messages appear:

```
C4K_WATCHDOG-3-CHILDFAILURE:
C4K_LINECARD-3-INTERRUPTDELAYED:
C4K_LINECARD-3-INTERRUPTCOMPLETED:
```

  Workaround: Eliminate link flap.

  Provide temporary remediation with a forced supervisor engine switchover. CSCtt06131

- After booting a switch with Supervisor Engine 7-E, you observe two versions of incorrect up time when using **show version** or **show redundancy**:

  Scenario #1: Display 136 years, 10 weeks, 6 hours, 26 minutes

```
Current Processor Information :
-------------------------------

Active Location = slot 5
        Current Software state = ACTIVE
       Uptime in current state = 136 years, 10 weeks, 6 hours, 26 minutes
                 Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3
Switch Software (cat4500e-UNIVERSALK9-M), Version 03.01.01.SG RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 14-Dec-10 22:12 by prod
               BOOT = bootflash:cat4500e-universalk9.SPA.03.01.01.SG.150-1.XO1.bin,1;
        Configuration register = 0x2102
```

  Scenario #2: Display “0 minute” after being up for a few days

```
Current Processor Information :
-------------------------------
               Active Location = slot 6
        Current Software state = ACTIVE
       Uptime in current state = 0 minute
```

```
                  Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3
Switch Software (cat4500e-UNIVERSALK9-M), Version 03.01.01.SG RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 14-Dec-10 22:12 by prod
                BOOT = bootflash:cat4500e-universalk9.SPA.03.01.01.SG.150-1.XO1.bin,1;
        Configuration register = 0x2102
```

Workaround: None. CSCtr54218

- Occasionally, when an interface with a QoS policy changes speed or when a QoS policy is being programmed on an interface, a Supervisor Engine 7 might unexpectedly encounter an FFM crash.

  Workaround: None. CSCtn81726

- A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

Note The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each 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 vulnerabilities in the March 2012 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_mar12.html

CSCtr28857

- Rarely, an FFM crash may occur when control plane queues are slow to empty.

  Workaround: None. CSCtr07852

- If a Supervisor Engine 7E is running Cisco IOS Release 3.2.2SG and a considerable quantity of simultaneous ACL, QoS, or Layer 3 programming occurs (usually on switch bootup), ACL, QoS and Layer 3 changes fail to take effect from that point forward.

  Workaround: None. The supervisor engine must be reloaded or failed over. CSCtw93728

- On a redundant system consisting of supervisor engines 6-E and 7-E, when the system consumes 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 Supervisor Engine 6-E to match that of Supervisor Engine 7-E.

- If you use Supervisor Engine 7E or Supervisor Engine 7L-E and you enter either the **show redundancy** or commands beginning with the keyword **redundancy**, the following error displays:

  ```
  Failed to find pr_handlers by uri
  ```

  .**Workaround**: None. A reload is required to restore these commands. CSCtw95861

- When you execute the **show flow monitor** *monitor_name params* **top** *number* command simultaneously from different terminals to display the top flows, the supervisor engine might crash.

  Workaround: Avoid entering flexible netflow **show** commands from more than one terminal, when you want to display the top flows. CSCtw61872

- After a switch reestablishes a lost connection with AAA servers configured for broadcast accounting, the switch crashes.

  Workaround: Do not use the **broadcast** keyword in the aaa accounting configuration. CSCts56125

- A switch configured with 802.1X might shows considerable CPU usage by the 802.1X switch process and displays the following message:

  ```
  SYS-2-MALLOCFAIL messages, and - on redundant systems - begins logging EM-4-SENDFAILED
  messages,
  ```

  The occurs under the following conditions:

  - Multi-auth (or multi-host) and MAB dot1x are configured on a port.
  - A voice VLAN is not configured on the port.
  - The device authenticates through 802.1X.
  - The connected device sends no traffic, falls over to MAB, and then successfully authenticates through 802.1X.
  - A dynamic VLAN is assigned to the port following 802.1X authorization.

  Workarounds:

  - Enter **shut** then **no shut** on the port to halt the high CPU and log messages.
  - Enter the **switchport voice vlan** command on the port. CSCtw73754

- If PoE linecards are present and you enter either the **show power inline module** *x* or **show power inline module** *x* **detail** command, very rarely the supervisor engine might crash.

  Workaround: None. CSCtx25697

- After a few hours of operation, during which DHCP is enabled and sessions receive DHCP information from a RADIUS server, a Cisco ASR router running as an LNS box crashes with DHCP related errors.

  Workaround: None. CSCtj48387

- Configuring an interface as uni-directional 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 bi-directional mode.

  Workaround: None. CSCtx95359

- If a switch is configured with the **aaa accounting send stop-record authentication failure** command, and MAB fails on the port and subsequent attempts are made to authorize the device after the restart timer expires, a high level of memory usage due to the "MAB Framework" process is observed.

  Workaround: Unconfigure the following from the switch: **aaa accounting send stop-record authentication failure**. CSCtj69212

- If REP is configured on a dot1q trunk and the native VLAN is administratively set to a non-default value, REP packets are not sent on the native VLAN.

  Workaround: Retain the trunk native V LAN as 1. CSCud05521

- SFP modules GLC-SX-MMD and GLC-SH-LMD may not be recognized when used with the WS-X4448-GB-SFP linecard.

  Workarounds:

  - Use modules GLC-SX-MM and GLC-LH-SM instead.
  - Use a release other than IOS XE 3.2.0SG (or IOS 15.0(2)SG) through IOS XE 3.2.6SG (or IOS 15.0(2)SG6). CSCub52430
  -

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

  Workaround: Shorten the dACL name. CSCug78653

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

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

  CSCue62019

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

  - A fast stream of traffic matches the URL redirect ACL as IPDT clears an address.
  - A traffic stream matches the URL redirect ACL and no URL redirect policy is installed for that IP address.

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

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

- If a device is authenticating while the RADIUS server goes down, the port connected to the device may enter the err-disabled state.

  Workaround: Configure RADIUS test and dead criteria.

  Example:

  ```
  radius-server dead-criteria time 10 tries 2
  radius-server host <ip> test username test key <key>
  radius-server deadtime 10
  ```

  CSCtn92693

- An SNMP walk of the LLDP MIB (OID 1.0.8802.1.1.2.1.5.4795) times out and produces a message similar to the following:

  ```
  Jun 19 10:48:51.835 UTC: %SYS-3-CPUHOG: Task is running for (2016)msecs, more than
  (2000)msecs (5/5),process = SNMP ENGINE.
  ```

  Workaround: Exclude the mib "lldpXMedMIB" with the **snmp-server view restrict lldpXMedMIB excluded** command. CSCuh88726

Resolved Caveats for Cisco IOS XE Release 3.2.0SG

This section lists the resolved caveats for Cisco IOS XE Release 3.2.0SG:

- On a redundant configuration, if a switchover occurs immediately after a port falls back to Webauth from 802.1X or MAB, you may notice a delay in loading the Webauth login page on the browser.

  Workaround: Enter **shut,** then **no-shut** on the link, then flush the IP device tracking table.

  CSCtc99174
- The **ip igmp snooping** command is not visible in VLAN range mode.

  Workaround: IGMP snooping can still be disabled on VLANs individually. CSCth17903
- When you attempt to copy from slaveusb0: or to slaveusb0:, the following message displays:

```
Copy in
progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCC
%Error reading slaveusb0:realtest (Error Sending Request)
```

  Workaround: Avoid remote copying to or from a standby usb0:. Copy from a standby bootflash or make a local copy directly at the standby bootflash. CSCti29518
- On all redundant configurations, RF Switchover History time is incorrect when accessed through cRFHistorySwactTime.

  Workaround: Use the **show redundancy** and **show redundancy states** commands to retrieve the switchover history times. CSCti53834
- On all redundant configurations, SNMP operations to obtain Redundancy Switchover history using cRFHistoryTable fail, displaying the following message:

```
"NO_SUCH_INSTANCE_EXCEPTION."
```

  Workaround: Enter the **show redundancy switchover history** command to obtain redundancy switchover history. CSCti55424
- The ciscoFlashPartitionFileCount object returns an incorrect file count for bootflash:, usb0:, slot0:, slaveslot0:, slavebootflash:, and slaveusb0:.

  Workaround: Use the **dir** *device* command to obtain the correct file count (for example, **dir bootflash:**). CSCti74130
- When you try to copy to slaveusb0: from the active bootflash, the following message displays:

```
%Error writing slaveusb0:/cat4500e-universalk9-lite.SSA.0.DEV-0.0.DEV-0.bin (Error
Sending Request)
 *Jul 30 11:38:58.890 UTC: %IOSXE-3-PLATFORM: STANDBY:4 kernel: usb 1-2: device
descriptor read/64, error -110
*Jul 30 11:39:14.169 UTC: %IOSXE-3-PLATFORM: STANDBY:4 kernel: usb 1-2: device
descriptor read/64, error -110
 *Jul 30 11:39:29.625 UTC: %IOSXE-3-PLATFORM: STANDBY:4 kernel: usb 1-2: device
descriptor read/64, error -110
```

  Workaround: Remove the slaveusb0, reinsert the slaveusb0:, then recopy. CSCti19321
- Three to five minutes after you create a GRE tunnel between interfaces on two switches (first hop and last hop), you observe that the FHR begins to drop the tunnel traffic. This causes the (S,G) entry, originally created on the LHR when sending IPv6 source traffic, to time out.

  Workaround: Enter **shut**, then **no shut** on the host port interface of the first hop. CSCti44397

- If you are using a large customized Web Authentication login page on a switch running Cisco IOS Release 12.2(53)SG3 or IOS XE 3.1.0 SG and multiple users attempt to access custom HTML pages, the switch might reload.

  Workaround: Unconfigure the customized HTML page to use default internal Webauth pages, change the configuration, then reload the switch. CSCti81874

- The Policy Based Routing (PBR) function fails on a Supervisor Engine 7-E running Cisco IOS Release 3.2.1.SG. Packets are software switched and not sent to the next hop as defined in the PBR route-map. Packets are routed to their destination via the IP routing table lookup rather than the route-map configured on the ingress interface.

  The **show platform hardware acl in entries vlan** command indicates that the ACL action does not point to an adjacency for the affected VLAN(s).

  Workaround: Enter the **cef table output-chain build favor memory-utilization** command globally. CSCtn91576

- When kron initiates a write to the startup-config (that is, execution of the **write mem** command), it is locked indefinitely.

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

  Workaround: Reload the switch to restore access, then use EEM with the timer event to schedule the required task. CSCtk68692

- If a redirect ACL is installed on multiple ports using cisco-av-pair url-redirect-acl=ACLNAME and you modify the ACL, the EPM MAIN process reports elevated CPU usage.

  Workaround: None. CSCtn61307

- If host mode multi-domain is configured, after a successful authorization, neither the data device nor the IP phone will pass traffic.

  Workaround: None. CSCtj56811

- A non-supplicant PC is connected to an 802.1x port in MDA mode. Upon no response to EAPOL, the PC is placed in a Guest VLAN (correct behavior). If the supplicant is enabled on the PC and the credentials are entered, the switch reports AUTHC success and AUTHZ fail. If client re-attempts 802.1x before the port returns to the Guest VLAN, this process succeeds.

  Workaround: None. CSCtl89361

- When a configuration file has VTP mode off and is copied to the running config, the VLANs that are not already in the VLAN database are not created.

  Workarounds:

  - Use VTP Mode transparent.
  - Create the VLANs manually. CSCtl94096

- LACP ports between a Catalyst 4500 Switch and a Nexus enter Suspended Mode when the native VLAN is tagged and changed to x on both chassis (native VLAN is not 1).

  Workaround: None. CSCtj90471

- LLDP frames are tagged incorrectly when leaving an 802.1q port if the native VLAN has a value other than 1.

  Workaround: Use the default native VLAN (VLAN of 1) for the trunks. CSCtn29321

- Some non-powered devices fail to linkup when connected to a 4648-RJ45-E/+E or 4748-RJ45+E line card port with a two-pair/4-wire cable (1,2,3,6).

This behavior is observed when you use IBM Cable Systems Type 1A/2A or any two-pair cable, including Cat5e.

Workaround:

- Use a four-pair wire.
- Enter the **power inline never** command.
- Enter the **speed auto 10 100** command. CSCtn43537

- Following a route flap, a Supervisor Engine 7-E running Cisco IOS XE Release 3.1.0XO or 3.1.1SG crashes and generates an FFM crashinfo file.

  Workaround: None. Upgrade to Cisco IOS XE Release 3.2.0SG or higher. CSCtr54723

Troubleshooting

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

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:

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:

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.

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