Release Notes for theCatalyst 4500 Series Switch, Cisco IOS Releases 15.0(2)SG

Current Release
15.0(2)SG11—October 18, 2016

Prior Release
15.0(2)SG10, 15.0(2)SG9, 15.0(2)SG8, 15.0(2)SG6, 15.0(2)SG5, 15.0(2)SG4, 15.0(2)SG3, 15.0(2)SG2, 15.0(2)SG1, 15.0(2)SG

These release notes describe the features, modifications, and caveats for Cisco IOS Release 15.0(2)SG on the Catalyst 4500 series switch.

Support for Cisco IOS Software Release 15.0(2)SG, 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

Note Although their *Release Notes* are unique, the 4 platforms (Catalyst 4500, Catalyst 4900, Catalyst ME 4900, and Catalyst 4900M/4948E) use the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide*.

For more information on the Catalyst 4500 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 the Cisco Catalyst 4500 Series Switch

The Enterprise Services image supports all Cisco Catalyst 4500 Series software features based on Cisco IOS Software, including enhanced routing. Customers planning to enable BGP for Supervisor Engine IV, V, or V-10GE will no longer need to purchase a separate BGP license (FR-IRC4) because BGP is included in the Enterprise Services package. Beginning with 12.2(53)SG2, we support the Enterprise Services image on Supervisor Engine 6L-E.

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).

Cisco IOS Release 12.2(46)SG1 introduced a new LAN Base software and an IP upgrade image. These complement the existing IP Base and Enterprise Services images. The LAN base image is supported on the Supervisor Engine II-Plus-10GE and Supervisor Engine 6L-E starting with Cisco IOS Release 12.2(52)XO. 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 Release 15.0(2)SG, on the Catalyst 4500 Series Switch, support for NEAT feature has been extended from IP Base to LAN Base and support for HSRP v2 IPV6 has been extended from Enterprise Services to IP Base.

Topics include:

Feature Support on the LAN Base vs IP Base Images

Table 1 is a detailed list of features supported on Catalyst 4500 Series Switch running Cisco IOS Software Release 15.0(2)SG. For the full list of supported features, check the Feature Navigator application:

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

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

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

Table 1 LAN Base/IP Base Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
2-way Community Private VLANs	No	Yes	Yes
8-Way CEF Load Balancing	No	Yes	Yes
10G Uplink Use	Yes	Yes	Yes
AAA Server Group	Yes	Yes	Yes
ACL Logging	Yes	Yes	Yes
All MIBs	Yes	Yes	Yes
ANCP Client	No	Yes	Yes
AppleTalk 1 and 2 (not supported on Sup 6-E and 6L-E)	No	No	Yes
Auto SmartPorts	Yes	Yes	Yes
AutoQoS	Yes	Yes	Yes
Auto-MDIX	Yes	Yes	Yes
Auto-Voice VLAN (part of Auto QoS)	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 Conditional Route Injection	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 Route-Map Continue	No	No	Yes
BGP Route-Map Continue Support for Outbound Policy	No	No	Yes
BGP Route-Map Policy List Support	No	No	Yes
BGP Soft Reset	No	No	Yes
Bidirectional PIM (IPv4 only)	No	Yes	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
BOOTP	Yes	Yes	Yes
Bootup GOLD	No	Yes	Yes
Broadcast/Multicast Suppression	Yes	Yes	Yes
Call Home	No	Yes	Yes
CDP/CDPv2	Yes	Yes	Yes
CFM	Yes	Yes	Yes
CGMP - Cisco Group Management Protocol	Yes	Yes	Yes
Cisco TrustSec SGT Exchange Protocol (SXP) IPv4	No	Yes	Yes
CiscoView Autonomous Device Manager (ADP)	Yes	Yes	Yes
CNS	Yes	Yes	Yes
Command Scheduler (Kron)	Yes	Yes	Yes
Community PVLAN support	No	Yes	Yes
Configuration File	Yes	Yes	Yes
Configuration Replace and Configuration Rollback	Yes	Yes	Yes
Configuration Rollback Confirmed Change	No	No	No
Copy Command	Yes	Yes	Yes
Console Access	Yes	Yes	Yes
Control Plane Policing (CoPP)	Yes	Yes	Yes
CoS to DSCP Map	Yes	Yes	Yes
CPU Optimization for Layer 3 Multicast Control Packets	Yes	Yes	Yes
Crashdump Enhancement[1]	Yes	Yes	Yes
DAI (Dynamic ARP Inspection)	Yes	Yes	Yes
DBL (Dynamic Buffer Limiting) - Active Queue Management	Yes	Yes	Yes
Debug Commands	Yes	Yes	Yes
Device Management	Yes	Yes	Yes
DHCP DHCPv6 Relay Agent notification for Prefix Delegation	No	Yes	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
DHCP Client	Yes	Yes	Yes
DHCP Server	Yes	Yes	Yes
DHCP Snooping	Yes	Yes	Yes
DHCPv6 Ethernet Remote ID option	Yes	Yes	Yes
Diagnostics Tools	Yes	Yes	Yes
Digital Optical Monitoring (DOM)	Yes	Yes	Yes
Downloading Software	Yes	Yes	Yes
DSCP to CoS Map	Yes	Yes	Yes
DSCP to egress queue mapping	Yes	Yes	Yes
Duplication Location Reporting Issue	No	Yes	Yes
EIGRP	No	No	Yes
EIGRP Stub Routing	No	Yes	Yes
Embedded Event Manager (EEM) 3.2	No	Yes	Yes
Embedded Event Manager and EOT integration	No	Yes	Yes
EnergyWise	Yes	Yes	Yes
EPoE	Yes	Yes	Yes
EtherChannel	Yes	Yes	Yes
Ethernet Management Port (Fa1 interface)[2]	Yes	Yes	Yes
Ethernet Operations, Administration, and Maintenance (OAM)	Yes	Yes	Yes
Event Log	Yes	Yes	Yes
Factory Default Settings	Yes	Yes	Yes
FHRP Enhanced Object Tracking of IP SLAs	No	No	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
File Management	Yes	Yes	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
Flex Links+(VLAN Load balancing)	Yes	Yes	Yes
Gateway Load Balancing Protocol (GLBP)	No	Yes	Yes
HSRP - Hot Standby Router Protocol	No	Yes	Yes
HTTP TA+A54CAC+ Accounting support	No	No	No
ID 4.0 Voice Vlan assignment	Yes	Yes	Yes
ID 4.1 Filter ID and per use ACL	Yes	Yes	Yes
IEEE 802.1ab LLDP (Link Layer Discovery Protocol)	Yes	Yes	Yes
IEEE 802.1ab LLDP/LLDP-MED	Yes	Yes	Yes
IEEE 802.1ab LLDP enhancements (PoE+Layer 2 COS)	Yes	No	No
IEEE 802.1ag D8.1 standard Compliant CFM, Y.1731 multicast LBM / AIS / RDI / LCK, IP SLA for Ethernet	Yes	Yes	Yes
IEEE 802.1p Support	Yes	Yes	Yes
IEEE 802.1p prioritization	Yes	Yes	Yes
IEEE 802.1p/802.1q	Yes	Yes	Yes
IEEE 802.1Q Tunneling	Yes	Yes	Yes
IEEE 802.1Q VLAN Trunking	Yes	Yes	Yes
IEEE 802.1s - Multiple Spanning Tree (MST) Standard Compliance	Yes	Yes	Yes
IEEE 802.1w Spanning Tree Rapid Reconfiguration	Yes	Yes	Yes
IEEE 802.1x (Auth-Fail VLAN, Accounting)	Yes	Yes	Yes
IEEE 802.1x Critical Authorization for Voice and Data	Yes	Yes	Yes
IEEE 802.1x Flexible Authentication	Yes	Yes	Yes
IEEE 802.1x with Multiple authenticated, multi-host	Yes	Yes	Yes
IEEE 802.1x Open Authentication	Yes	Yes	Yes
IEEE 802.1x User Port Description	Yes	Yes	Yes
IEEE 802.1x VLAN Assignment)	Yes	Yes	Yes
IEEE 802.1x Wake on LAN	Yes	Yes	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
IEEE 802.1x Agentless Audit 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 MIB Support	Yes	Yes	Yes
IEEE 802.1x Multi-Domain Auth with Voice VLAN Assignment	Yes	Yes	Yes
IEEE 802.1x Multi-Domain Auth	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 and MAB with ACL assignment	Yes	Yes	Yes
IEEE 802.3ad Link Aggregation (LACP)	Yes	Yes	Yes
IEEE 802.3ad Link Aggregation (LACP) Port-Channel Standalone Disable	Yes	Yes	Yes
IEEE 802.3ah and CFM Interworking	No	Yes	Yes
IEEE 802.3x Flow Control	Yes	Yes	Yes
IEEE 802.1x Web-Auth	Yes	Yes	Yes
IGMP Filtering	Yes	Yes	Yes
IGMP Querier	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
Ingress Policing	Yes	Yes	Yes
Interface Access (Telnet, Console/Serial, Web)	Yes	Yes	Yes
IP Enhanced IGRP Route Authentication	No	No	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
IP Event Dampening	Yes	Yes	Yes
IP Multicast Load Splitting across Equal-Cost Paths	No	Yes	Yes
IP Named Access Control List	Yes	Yes	Yes
IP over IPv6 Tunnels	Yes	Yes	Yes
IP Routing	Yes	Yes	Yes
IP SLAs DHCP Operation	No	No	Yes
IP SLAs Distribution of Statistics	No	No	Yes
IP SLAs DNS Operation	No	No	Yes
IP SLAs FTP Operation	No	No	Yes
IP SLAs History Statistics	No	No	Yes
IP SLAs 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 SNMP Support	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

Table 1 LAN Base/IP Base Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
IP SLAs Sub-millisecond Accuracy Improvements	No	NO	Yes
IPSG (IP Source Guard) v4	Yes	Yes	Yes
IPSG (IP Source Guard) v4 for Static Hosts	Yes	Yes	Yes
IP Unnumbered for VLAN-SVI interfaces	No	Yes	Yes
IPv6 (Internet Protocol Version 6)	Yes	Yes	Yes
IPv6 HSRP	No	Yes	Yes
IPv6 IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	No	No	Yes
IPV6 MLD snooping V1 and V2	Yes	Yes	Yes
IPv6 Multicast	No	Yes	Yes
IPv6 Multicast: Bootstrap Router (BSR)	No	No	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 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 Neighbor Discovery	No	Yes	Yes
IPV6 Reformation	NA	Yes	Yes
IPV6 Router Advertisement (RA) Guard	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
ISIS for IPv4 and IPv6	No	No	Yes
ISL Trunk	Yes	Yes	Yes
ISSU (IOS In-Service Software Upgrade)	No	Yes	Yes
Jumbo Frames	Yes	Yes	Yes
Layer 2 Debug	Yes	Yes	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
Layer 2 Protocol Tunneling (L2PT)	Yes	Yes	Yes
Layer 2 Traceroute	Yes	Yes	Yes
Layer 3 Multicast Routing (PIM SM, SSM, Bidir)	No	Yes	Yes
Link State Tracking	Yes	Yes	Yes
Local Web Auth	Yes	Yes	Yes
MAB (MAC Authentication Bypass) for Voice VLAN	Yes	Yes	Yes
MAC Address Filtering	Yes	Yes	Yes
MAC Based Access List	Yes	Yes	Yes
Management IPV6 port	Yes	Yes	Yes
Multicast BGP (MBGP)	No	No	Yes
Multicast Routing Monitor (MRM)	No	No	Yes
Multicast Source Discovery Protocol (MSDP)	Yes	Yes	Yes
Multi-authentication and VLAN Assignment	Yes	Yes	Yes
Multi-VRF Support (VRF lite)	No	No	Yes
NAC - L2 IEEE 802.1x	Yes	Yes	Yes
NAC - L2 IP	Yes	Yes	Yes
NEAT Enhancement: Re-Enabling BPDU Guard Based on User Configuration	Yes	Yes	Yes
Network Edge Access Topology (NEAT)	Yes	Yes	Yes
Network Time Protocol (NTP)	Yes	Yes	Yes
Time Protocols (SNTP, TimeP) master	Yes	Yes	Yes
No. of QoS Filters No. of Security ACE	Yes (4K entries)	Yes	Yes
No. of VLAN Support	2048	4096	4096
NSF - BGP	No	No	Yes
NSF - EIGRP	No	No	Yes
NSF - OSPF v2	No	No	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
NSF/SSO (Nonstop Forwarding with Stateful Switchover)	No	No	Yes
On Demand Routing (ODR)	No	No	Yes
OSPF	No	Yes[3]	Yes
OSPF Flooding Reduction	No	Yes[4]	Yes
OSPF for Routed Access	No	Yes	Yes
OSPF Incremental Shortest Path First (i-SPF) Support	No	Yes[5]	Yes
OSPF Link State Database Overload Protection	No	Yes[6]	Yes
OSPF Not-So-Stubby Areas (NSSA)	No	Yes[7]	Yes
OSPF Packet Pacing	No	Yes[8]	Yes
OSPF Shortest Paths First Throttling	No	Yes[9]	Yes
OSPF Stub Router Advertisement	No	Yes[10]	Yes
OSPF Support for Fast Hellos	No	Yes[11]	Yes
OSPF Support for Link State Advertisement (LSA) Throttling	No	Yes[12]	Yes
OSPF Support for Multi-VRF on CE Routers	No	Yes[13]	Yes
OSPF Update Packet-Pacing Configurable Timers	No	Yes[14]	Yes
Out-of-band Management Port	Yes	Yes	Yes
PAgP	Yes	Yes	Yes
Passwords Password clear protection	Yes	Yes	Yes
Per-User ACL Support for 802.1X/MAB/Webauth users	Yes	Yes	Yes
PIM Sparse Mode Version4	No	No	Yes
PIM Version 1	No	Yes	Yes
PM Version 2	No	Yes	Yes
PoE (up to 15.4W only)	Yes	Yes	Yes
PoE+ Ready	Yes	Yes	Yes
Policy-Based Routing (PBR)	No	No	Yes
Port Access Control List (PACL)	Yes	Yes	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
Port Monitoring (interface Stats)	Yes	Yes	Yes
Port Security	Yes	Yes; only 1024 MACs	Yes
Post Status	Yes	Yes	Yes
Pragmatic General Multicast (PGM)	Yes	Yes	Yes
Private VLANs	Yes	Yes	Yes
Propagation of Location Info over CDP	Yes	Yes	Yes
PVLAN over EtherChannel	Yes	Yes	Yes
PVST+ (Per Vlan Spanning Tree Plus)	Yes	Yes	Yes
Q-in-Q	No	Yes	Yes
RACL (DSCP based)	Yes	Yes	Yes
RADIUS/TACACS+ (AAA)	Yes	Yes	Yes
RADIUS Attribute 44 (Accounting Session ID) in Access Requests	Yes	Yes	Yes
Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)	Yes	Yes	Yes
Remote SPAN (RSPAN)	Yes	Yes	Yes
REP Resilient Ethernet Protocol)	Yes	Yes	Yes
REP No Edge Neighbour Enhancement	Yes	Yes	Yes
RIP v1	No	Yes	Yes
RMON	Yes	Yes	Yes
Role-Based Access Control CLI commands (RBAC)	Yes	Yes	Yes
RPR	Yes	Yes	Yes
RPVST+	Yes	Yes	Yes
RSPAN	Yes	Yes	Yes
Secure Copy (SCP)	Yes	Yes	Yes
Secure Shell SSH Version 1, 2 Server Support	Yes	Yes	Yes
Secure Shell SSH Version 1, 2 Client Support	Yes	Yes	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
Service Advertisement Framework (SAF)	No	No	Yes
SmartPorts (Role based MACRO)	Yes	Yes	Yes
SNMP (Simple Network Management Protocol)	Yes	Yes	Yes
SNMPv3 (SNMP Version 3)	Yes	Yes	Yes
Source Port Filtering (Private VLAN)	Yes	Yes	Yes
Source Specific Multicast (SSM)	No	Yes	Yes
Source Specific Multicast (SSM) - IGMPv3,IGMP v3lite, and URD	Yes	Yes	Yes
Source Specific Multicast (SSM) Mapping	Yes	Yes	Yes
SPAN (# of sessions) – Port Mirroring	Yes (2 bidirectional sessions)	Yes (8 bidirectional sessions)	Yes (8 bidirectional sessions)
SSHv2/Secure Copy, FTP, SSL, Syslog, Sys Information	Yes	Yes	Yes
SSO (Stateful SwitchOver)	No	Yes	Yes
Static Routing (IPv4/IPv6)	Yes	Yes	Yes
Storm Control - Per-Port Multicast Suppressio	Yes	Yes	Yes
Stub IP Multicast Routing	No	Yes	No
SVI (Switch Virtual Interface) Autostate Exclude	Yes	Yes	Yes
TACACS+	Yes	Yes	Yes
Time-Based Access Lists	Yes	Yes	Yes
Time Domain Reflectometry (TDR)	No	Yes	Yes
Time Protocols (SNTP, TimeP)	Yes	Yes	Yes
Traffic Mirroring (SPAN)	Yes	Yes	Yes
Trusted Boundary (LLDP & CDP Based)	Yes	Yes	Yes
Unicast Reverse Path Forwarding (uRPF)	Yes	Yes	Yes
UniDirectional Link Detection (UDLD)	Yes	Yes	Yes
Virtual Router Redundancy Protocol (VRRP)	No	Yes	Yes
VLAN Access Control List (VACL)	Yes	Yes	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
VLAN Mapping (VLAN Translation)	Yes	Yes	Yes
Voice VLAN	Yes	Yes	Yes
VTP (Virtual Trunking Protocol) Version 2	Yes	Yes	Yes
VTP version 3	Yes	Yes	Yes
WCCP Redirection on Inbound Interfaces	No	Yes	Yes
WCCP Version 2	No	Yes	Yes
XML-PI	Yes	Yes	Yes

[1] Supported only on Supervisor Engine 6-E and Supervisor Engine 6L-

[2] Starting with Cisco IOS Release 12.2(46)SG

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

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

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

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

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

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

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

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

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

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

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

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

Note You can purchase a special license to enable the 10 Gigabit uplinks in the LAN Base image without moving to IP Base.

Features Unique to Supervisor Engines 6-E and 6L-E

With Cisco IOS Release 15.0(2)SG, the following features are available only with Supervisor Engine 6-E and Supervisor Engine 6L-E:

- ARP QoS
- IPv6
  - IPv6 Addressing Architecture
  - CDP IPv6 Address Family
  - DNS resolver for AAAA over an IPv4 transport
  - DNS resolver for AAAA over an IPv6 transport
  - Extended ACL

  - Hop-by-Hop option header
  - ICMP Rate Limiting
  - ICMPv6
  - ICMPv6 Redirect
  - IPv6 over IEEE 802.1Q
  - ISATAP (supported in software only)
  - Loopback
  - MLD Snooping (supported in software and hardware on Catalyst 4900M, Catalyst 4948E, Supervisor Engine 6-E, and Catalyst 6L-E)
  - MLDv1/v2
  - MTU Path Discovery for IPv6
  - OSPFv3
  - RIPng
  - EIGRPv6
  - PACL
  - RA Guard
  - IPv6 Interface Statistics
  - QoS
- QoS
  - Two Rate three Color Policing
  - Table map support for marking
  - Class based queuing actions (shaping/bandwidth/queue-limit/dbl/strict priority)
- QoS for IPv6
- Voltage Margining CLI

Unsupported Features

For all Supervisor Engines (II-Plus thru 6-E), the following features are not supported in Cisco IOS Release 15.0(2)SG for the Catalyst 4500 series switches:

- The following ACL types:
  - Standard Xerox Network System (XNS) access list
  - Extended XNS access list
  - DECnet access list
  - Protocol type-code access list
- ADSL and Dial access for IPv6
- AppleTalk EIGRP (use native AppleTalk routing instead)
- Bridge groups
- CEF Accounting

- Cisco IOS software IPX ACLs:
  - <1200-1299> IPX summary address access list
- Cisco IOS software-based transparent bridging (also called “fallback bridging”)
- Connectionless (CLNS) routing; including IS-IS routing for CLNS. IS-IS is supported for IP routing only.
- DLSw (data-link switching)
- IGRP (use EIGRP instead)
- **isis network point-to-point** command
- Kerberos support for access control
- LLDP HA
- Lock and key
- NAT-PT for IPv6
- Netflow per-VRF
- PBR with Multiple Tracking Options
- QoS for IPv6 traffic (only supported on Supervisor 6)
- Reflexive ACLs
- Routing IPv6 over an MPLS network
- WCCP version 1
- CFM CoS
- PBR with EOT

Orderable Product Numbers

Table 2 Orderable Product Numbers for the Catalyst 4500 Series Switch

Product Number	Description	Image
S45LB-15002SG(=)	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine II-Plus-10GE (LAN Base image)	cat4500-lanbase-mz
S45LBK9-15002SG(=)	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine II-Plus-10GE (LAN Base image with 3DES)	cat4500-lanbasek9-mz
S45IPBU-15002SG(=)	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine II-Plus-10GE (IP Base Upgrade image)	Cat4500-ipbase-mz
S45IPBUK9-15002SG(=)	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine II-Plus-10GE (IP Base Upgrade image with 3DES)	Cat4500-ipbasek9-mz
S45IPB-15002SG(=)	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image without Crypto)	Cat4500-ipbase-mz

Table 2 Orderable Product Numbers for the Catalyst 4500 Series Switch

Product Number	Description	Image
S45IPBK9-15002SG(=)	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image with Triple Data Encryption Standard [3DES])	Cat4500-ipbasek9-mz
S45ES-15002SG(=)	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with Border Gateway Protocol (BGP) support, without Crypto)	Cat4500-entservices-mz
S45ESK9-15002SG(=)	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with 3DES and BGP support)	Cat4500-entservicesk9-mz
S45EIPB-15002SG(=)	Cisco IOS Software for the Cisco Catalyst 4500 Supervisor Engine 6-E and Sup6L-E and the Catalyst4948E (IP Base image)	Cat4500e-ipbase-mz
S45EIPBK9-15002SG(=)	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine 6-E and Sup6L-E and the Catalyst4948E (IP Base image with 3DES)	Cat4500e-ipbasek9-mz
S45EES-15002SG(=)	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine 6-E and Sup6L-E and the Catalyst4948E (Enterprise Services image)	Cat4500e-entservices-mz
S45EESK9-15002SG(=)	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine 6-E and Sup6L-E and the Catalyst4948E (Enterprise Services image with 3DES)	Cat4500e-entservicesk9-mz
S45EESU-15002SG(=)	Cisco IOS Enterprise image upgrade from LAN Base for the Supervisor 6-E and Supervisor 6L-E	Cat4500e-entservices-mz
S45EESUK915002SG(=)	Cisco IOS Enterprise with 3DES upgrade from LAN Base for the supervisor 6-E and Supervisor 6L-E	Cat4500e-entservicesk9-mz
S45EIPBU-15002SG(=)	Cisco IOS Software for the Catalyst 4500 Series Supervisor Engine 6-E and Sup6L-E , Catalyst4948E IOS IP Base Upgrade	Cat4500e-ipbase-mz
S45EIBUK9-15002SG(=)	Cisco IOS Software for the Catalyst 4500 Series Supervisor Engine 6-E and Sup6L-E , Catalyst4948E IOS IP Base Upgrade SSH	Cat4500e-ipbasek9-mz

Cisco Classic IOS Release Strategy for the Catalyst 4500 Series Switch

Cisco IOS Release 15.0SG train offers the latest features for the Catalyst 4500 Series supervisor engines. If you need the latest hardware support and software features you should migrate to Cisco IOS Release 15.0(2)SG.

Catalyst 4500 Series has two maintenance trains. Cisco IOS Release 12.2(53)SG4 is the recommended release for customers who require a release with a maintenance train. This release includes support for the WS-X45-Sup6L-E supervisor engine and OSPF for routed Access. Cisco IOS Release 15.0(2)SG is the latest maintenance train base.

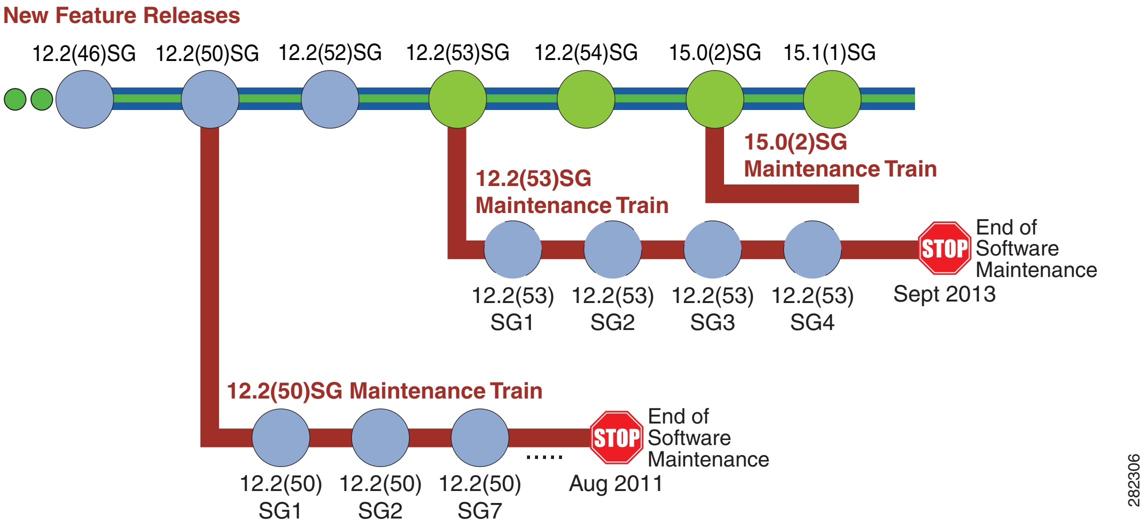
For more information on the Catalyst 4500 series switches, visit the following URL:

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

Cisco IOS Software Migration Guide

Figure 1 displays the two active trains, 12.2(53)SG and 15.0(2)SG.

Figure 1 Software Release Strategy for the Catalyst 4500 Series Switch



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

System Requirements

This section describes the system requirements:

- Supported Hardware on Catalyst 4500 Series Switch, page 19
- Supported Hardware on Catalyst 4500 E-Series Switch, page 23
- Features Unique to Supervisor Engines 6-E and 6L-E, page 14
- Unsupported Features, page 15

Supported Hardware on Catalyst 4500 Series Switch

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

Table 3 Supported Hardware

Product Number (append with "=" for spares)	Product Description	Software Release
		Minimum
Supervisor Engines		
WS-X4013+=	Catalyst 4500 series switch Supervisor Engine II-Plus **Note** This engine is supported only on 3, 6, and 7 slot chassis (not on 10-slot chassis).	12.1(19)EW
WS-X4013+TS	Catalyst 4500 series switch Supervisor Engine II-Plus-TS **Note** This engine is supported only on 3 slot chassis.	12.2(20)EWA
WS-X4013+10GE	Catalyst 4500 series switch Supervisor Engine II-Plus-10GE **Note** This engine is supported only on 3, 6, and 7 slot chassis (not on 10-slot chassis).	12.2(25)SG
WS-X4515=	Catalyst 4500 series switch Supervisor Engine IV	12.1(12c)EW
WS-X4515/2=	Catalyst 4507R series switch Redundant Supervisor Engine IV	12.1(12c)EW
WS-X4516=	Catalyst 4500 series switch Supervisor Engine V	12.2(18)EW
WS-X4516/2=	Catalyst 4507R series switch Redundant Supervisor Engine V	12.2(18)EW
WS-X4516-10GE=	Catalyst 4500 series switch Supervisor Engine V-10GE	12.2(25)EW
WS-X45-Sup6-E	Catalyst 4500 E-series switch Supervisor Engine 6-E **Note** This engine is supported on legacy and E-series chassis.	12.2(40)SG
WS-X45-Sup6L-E	Catalyst 4500 E-series switch Supervisor Engine 6L-E **Note** This engine is supported on legacy and E-series 3,6, and 7 slot chassis.	12.2(52)XO
Gigabit Ethernet Switching Modules		
WS-X4302-GB	2-port 1000BASE-X (GBIC) Gigabit Ethernet module	12.1(19)EW
WS-X4306-GB	6-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	12.1(8a)EW
WS-X4418-GB	18-port 1000BASE-X (GBIC) Gigabit Ethernet server switching module	12.1(8a)EW
WS-X4412-2GB-T	12-port 1000BASE-T Gigabit Ethernet and 2-GBIC ports switching module	12.1(8a)EW
WS-X4424-GB-RJ45	24-port 10/100/1000BASE-T Gigabit Ethernet RJ-45 switching module	12.1(8a)EW
WS-X4448-GB-LX	48-port 1000BASE-LX (small form-factor pluggable) Gigabit Ethernet fiber optic interface switching module	12.1(8a)EW
WS-X4448-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet switching module	12.1(8a)EW
WS-X4448-GB-SFP	48-port 1000BASE-X (small form-factor pluggable) module	12.2(20)EW
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	12.2(20)EWA
WS-X4524-GB-RJ45V	24-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af	12.2(18)EW
WS-X4548-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet module	12.1(19)EW

Table 3 Supported Hardware (continued)

Product Number (append with “=” for spares)	**Product Description**	**Software Release**
		Minimum
WS-X4548-GB-RJ45V	48-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af	12.2(18)EW
WS-X4548-RJ45V+	48-port 10/100/1000 Premium PoE line card	12.2(50)SG
WS-X4624-SFP-E	Non-blocking 24-port 1000BASEX (small form factor pluggable) module	12.2(44)SG
WS-X4648-RJ45V-E	48 port 10/100/1000 Mb with 2 to 1 oversubscription	12.2(40)SG
WS-X4648-RJ45V+E	48 port 10/100/1000 Mb with 2 to 1 oversubscription	12.2(40)SG
Fast Ethernet Switching Modules		
WS-X4124-FX-MT	24-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module	12.1(8a)EW
WS-X4148-FX-MT	48-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module	12.1(8a)EW
WS-X4148-FE-LX-MT	48-port 100BASE-LX10 Fast Ethernet MT-RJ single-mode fiber switching module	12.1(13)EW
WS-X4148-FE-BD-LC	48-port 100BASE-BX10-D module	12.2(18)EW
WS-X4248-FE-SFP	48-port 100BASE-X SFP switching module	12.2(25)SG
WS-U4504-FX-MT	4-port 100BASE-FX (MT-RF) uplink daughter card	12.1(8a)EW
Ethernet/Fast Ethernet (10/100) Switching Modules		
WS-X4124-RJ45	24-port 10/100 RJ-45 module	12.2(20)EW
WS-X4148-RJ	48-port 10/100 RJ-45 switching module	12.1(8a)EW
WS-X4148-RJ21	48-port 10/100 4xRJ-21 (telco connector) switching module	12.1(8a)EW
WS-X4148-RJ45V	48-port Pre-standard PoE 10/100BASE-T switching module	12.1(8a)EW for data support 12.1(11b)EW for data and inline power support
WS-X4224-RJ45V	24-port 10/100BASE-TX RJ-45 Cisco Catalyst 4500 series PoE 802.3af	12.2(20)EW
WS-X4232-GB-RJ	32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	12.1(8a)EW
WS-X4248-RJ45V	48-port 10/100BASE-T RJ-45 Cisco Catalyst 4500 series PoE 802.3af	12.2(18)EW
WS-X4248-RJ21V	48-port 10/100 Fast Ethernet RJ-21 Cisco Catalyst 4500 series PoE 802.3af telco	12.2(18)EW
WS-X4232-RJ-XX	32-port 10/100 Fast Ethernet RJ-45 modular uplink switching module	12.1(8a)EW
Other Modules		
MEM-C4K-FLD64M	Catalyst 4500 series switch CompactFlash, 64 MB Option	12.1(8a)EW
MEM-C4K-FLD128M	Catalyst 4500 series switch CompactFlash, 128 MB Option	12.1(8a)EW
WS-F4531	Catalyst 4500 series switch Netflow Services Card on Catalyst 4500 series switch Supervisor Engines IV and V	12.1(13)EW
WS-X4590=	Catalyst 4500 series switch Fabric Redundancy Modules	12.2(18)EW

Table 3 Supported Hardware (continued)

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
PWR-C45-1000AC	Catalyst 4500 series switch 1000 Watt AC power supply for chassis 4503, 4506, and 4507R (data only)	12.1(12c)EW
PWR-C45-1400DC	Catalyst 4500 series switch 1400 Watt DC triple input power supply (data-only)	12.2(25)EW
PWR-C45-1400DC-P	Catalyst 4500 series switch 1400 Watt DC power supply with integrated PEM	12.1(19)EW
PWR-C45-1400AC	Catalyst 4500 series switch 1400 Watt AC power supply (data-only)	12.1(12c)EW
PWR-C45-1300ACV	Catalyst 4500 series switch 1300 Watt AC power supply with integrated voice for chassis 4503, 4506, and 4507R	12.1(12c)EW
PWR-C45-2800ACV	Catalyst 4500 series switch 2800 Watt AC power supply with integrated voice (data and PoE) for chassis 4503, 4506, and 4507R	12.1(12c)EW
PWR-C45-4200ACV	Catalyst 4500 series switch 4200 Watt AC dual input power supply with integrated voice (data and PoE)	12.2(25)EWA5
WS-P4502-1PSU	Catalyst 4500 series switch auxiliary power shelf (25-slot), including one PWR-4502	12.1(19)EW
PWR-4502	Catalyst 4500 series switch auxiliary power shelf redundant power supply	12.1(19)EW
PWR-C45-6000ACV	Catalyst 4500 Series Switch 6000 W AC power supply	12.2(53)SG

For Catalyst 4500 transciever module compatibility information, see the URL:

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

Table 4 briefly describes the four chassis in the Catalyst 4500 Series Switch. For the chassis listed in the table, refer to Table 7 on page 24 for software release information.

Table 4 Chassis Description for the Catalyst 4500 Series Switch

Product Number (append with "=" for spares)	**Description of Modular Chassis**
WS-C4503	Catalyst 4503 chassis includes these components: • 3 slots • Fan tray • Supports Supervisor Engine 6L-E, Supervisor Engine 6-E, Supervisor Engine V-10GE, Supervisor Engine V, Supervisor Engine IV, Supervisor Engine III, Supervisor Engine II-Plus-10GE, Supervisor Engine II-Plus-TS, Supervisor Engine II-Plus, and Supervisor Engine II
WS-C4506	Catalyst 4506 chassis includes these components: • 6 slots • Fan tray • Supports Supervisor Engine 6L-E, Supervisor Engine 6-E, Supervisor Engine V-10GE, Supervisor Engine V, Supervisor Engine IV, Supervisor Engine III, Supervisor Engine II-Plus-10GE, Supervisor Engine II-Plus, and Supervisor Engine II
WS-C4507R	Catalyst 4507R chassis includes these components: • 7 slots • Fan tray • Supports Supervisor Engine 6L-E, Supervisor Engine 6-E, Supervisor Engine V-10GE, Supervisor Engine V, Supervisor Engine IV, Supervisor Engine II-Plus-10GE, and Supervisor Engine II-Plus
WS-C4510R	Catalyst 4510R chassis includes these components: • 10 slots; slot 10 accepts only the Catalyst 4500 series 2-port Gigabit Ethernet line card (WS-X4302-GB with Supervisor Engine V) **Note** The Supervisor Engine V-10GE does not have this restriction. • Fan tray • Supports Supervisor Engine 6-E, Supervisor Engine V-10GE and Supervisor Engine V

Table 5 DOM Support on the Catalyst 4500 Series Switch

Transceiver Module	Support in Software Since...
CWDM- SFP-*xx*	12.2(20)EWA
DWDM-GBIC-*xx*	12.1(19)EW
DWDM-SFP	12.2(37)SG
DWDM-X2-*xx*	12.2(50)SG
GLC-BX-D	12.2(20)EWA
GLC-BX-U	12.2(20)EWA
SFP-10G-SR	12.2(54)SG
SFP-10G-LR	12.2(54)SG
SFP-10G-LRM	12.2(54)SG

Supported Hardware on Catalyst 4500 E-Series Switch

In addition to the classic line cards and supervisor engines, Cisco IOS Software Release 15.0(2)SG supports the next-generation high-performance E-Series Supervisor Engine 6-E with CenterFlex technology and E-Series line cards and chassis. A brief list of primary E-Series hardware supported on Catalyst 4500 series switch (Table 6).

Table 6 Supported E-Series Hardware

Product Number	Description
WS-C4503-E	Cisco Catalyst 4500 E-Series 3-Slot Chassis • Fan tray • No Power Supply
WS-C4506-E	Cisco Catalyst 4500 E-Series 6-Slot Chassis • Fan tray • No Power Supply
WS-C4507R-E	Cisco Catalyst 4500 E-Series 7-Slot Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability
WS-C4507R+E	Cisco Catalyst 4500 E-Series 7-Slot 48 GB-ready Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability

Table 6 Supported E-Series Hardware

Product Number	Description
WS-C4510R-E	Cisco Catalyst 4500 E-Series 10-Slot Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • Slots 8, 9, and 10 are limited to 6Gbps when used with a Supervisor Engine 6-E.
WS-C4510R+E	Cisco Catalyst 4500 E-Series 10-Slot 48 GB-ready Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • You cannot place a linecard with a backplane traffic capacity exceeding 6Gbps in slots 8, 9 and 10 of a Catalyst 4510R+E chassis when used with a Supervisor Engine 6-E.
WS-X45-Sup6-E	Cisco Catalyst 4500 E-Series Sup 6-E, 2x10GE(X2) w/ TwinGig
WS-X45-Sup6L-E	Cisco Catalyst 4500 E-Series Sup 6L-E
WS-X4624-SFP-E	Cisco Catalyst 4500 E-series 24-Port 1000BaseX (small form factor pluggable) module
WS-X4648-RJ45V-E	Cisco Catalyst 4500 E-Series 48-Port PoE 802.3af 10/100/1000(RJ45)
WS-X4648-RJ45V+E	Cisco Catalyst 4500 E-Series 48-Port Premium PoE 10/100/1000
WS-X4606-X2-E	Cisco Catalyst 4500 E-Series 6-Port 10GbE (X2) w/ TwinGig
WS-X4648-RJ45-E	Cisco Catalyst 4500 E-Series 48-Port 10/100/1000(RJ45)

Table 7 outlines the chassis and supervisor engine compatibility.
(M=Minimum release, R=Recommended release)

Table 7 Chassis and Supervisor Compatiblity

Chassis	Sup II+	Sup II+TS	Sup II+10G	Sup IV	Sup V	Sup V-10GE	Sup 6-E	Sup 6L-E
WS-C4503-E	M: 12.2(31)SGA6	M: 12.2(31)SGA6	M: 12.2(31)SGA6	M: 12.2(31)SGA6	M: 12.2(31)SGA6	M: 12.2(31)SGA6	M: 12.2(40)SG	M: 12.2(52)XO
WS-C4506-E	M: 12.2(31)SGA6		M: 12.2(31)SGA6	M: 12.2(31)SGA6	M: 12.2(31)SGA6	M: 12.2(31)SGA6	M: 12.2(40)SG	M: 12.2(52)XO
WS-C4507R-E	M: 12.2(31)SGA6		M: 12.2(31)SGA6	M: 12.2(31)SGA6	M: 12.2(31)SGA6	M: 12.2(31)SGA6	M: 12.2(40)SG	M: 12.2(52)XO
WS-C4507R+E	M: 12.2(54)SG		M: 12.2(54)SG	M: 12.2(54)SG	M: 12.2(54)SG	M: 12.2(54)SG	M: 12.2(54)SG	M: 12.2(54)SG
WS-C4510R-E					M: 12.2(31)SGA6	M: 12.2(31)SGA6	M: 12.2(40)SG	
WS-C4510R+E					M: 12.2(54)SG	M: 12.2(54)SG	M: 12.2(54)SG	

New and Changed Information

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

- New Hardware Features in Release 15.0(2)SG1, page 25
- New Software Features in Release 15.0(2)SG1, page 25
- New Hardware Features in Release 15.0(2)SG, page 25
- New Software Features in Release 15.0(2)SG, page 25

New Hardware Features in Release 15.0(2)SG1

Release 15.0(2)SG1 provides no new hardware on the Catalyst 4500 series switch.

New Software Features in Release 15.0(2)SG1

Release 15.0(2)SG1 provides the following new software feature on the Catalyst 4500 series switch.

- A new option for Layer 2 control plane QoS, **eapol**, enabling customers to police EAPLOL packets based on ethertype.
- IEEE 802.3ad Link Aggregation (LACP) Port-Channel Standalone Disable

New Hardware Features in Release 15.0(2)SG

Release 15.0(2)SG provides the following new hardware on the Catalyst 4500 series switch:

- SFP-10G-ER
- 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)

New Software Features in Release 15.0(2)SG

Release 15.0(2)SG provides the following new software features 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)
- 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)
- IEEE 802.1x Critical Authorization for Voice and Data (“Configuring 802.1X Port-Based Authentication 802.1X” chapter)
- Multi-authentication and VLAN Assignment (“Configuring 802.1X Port-Based Authentication

  802.1X” chapter)
- NEAT Enhancement: Re-Enabling BPDU Guard Based on User Configuration (“Configuring 802.1X Port-Based Authentication” 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)
- Resilient Ethernet Protocol-no-edge-neighbour-enhancement (“Configuring Resilient Ethernet Protocol” chapter)
- WCCP Version 2 (“Configuring WCCP Version 2 Services” chapter)

Upgrading the System Software

In most cases, upgrading the switch to a newer release of Cisco IOS software does not require a ROMMON upgrade. However, if you are running an early release of Cisco IOS software and plan to upgrade, refer to the following tables for the minimum Cisco IOS image and the recommended ROMMON release, respectively.

Note You must upgrade to at leaset ROMMON Release 12.2(44r)SG5 to run Cisco IOS Release 15.0(2)SG on the Supervisor Engine 6-E and Supervisor Engine 6L-E. 12.2(44r)SG9 is recommended.

Caution Most supervisor engines have the required ROMMON release. However, due to caveat CSCed25996, we recommend that you upgrade your ROMMON to the recommended release.

Table 8 Supervisor Engine and Recommended ROMMON Release

Supervisor Engine	Recommended ROMMON Release
IV	12.2(31r)SGA4
II-Plus	12.2(31r)SGA4
II-Plus-10GE	12.2(31r)SGA4

Table 8 Supervisor Engine and Recommended ROMMON Release

Supervisor Engine	Recommended ROMMON Release
V	12.2(31r)SGA4
II-Plus-TS	12.2(31r)SGA4
V-10GE	12.2(31r)SGA4
6-E	12.2(44r)SG9
6L-E	12.2(44r)SG9

Table 9 ROMMON Release and Promupgrade Programs

ROMMON Release	Promupgrade Program
12.2(31r)SGA4	cat4500-e-ios-promupgrade-122_31r_SGA4
12.2(44r)SG5	cat4500-e-ios-promupgrade-122_44r_SG5
12.2(44r)SG9	cat4500-e-ios-promupgrade-122_44r_SG9
12.2(44r)SG10	cat4500-e-ios-promupgrade-122_44r_SG10

The following sections describe how to upgrade your switch software:

- Identifying an +E Chassis and ROMMON, page 27
- Guidelines for Upgrading the ROMMON, page 28
- Upgrading the Supervisor Engine ROMMON from the Console, page 28
- Upgrading the Supervisor Engine ROMMON Remotely Using Telnet, page 31
- Upgrading the Cisco IOS Software, page 36

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.

Guidelines for Upgrading the ROMMON

Caution If your supervisor engine is shipped with a newer version of ROMMON then do not downgrade! The new ROMMON will have board settings based on a hardware revision of components, and old settings will not work.

Caution Upgrading ROMMON on Supervisor Engine 6-E and 6L-E may reset their uplink interfaces. Software prior to Cisco IOS Release 15.0(2)SG did not detect and recover from this situation when the standby supervisor engine ROMMON is upgraded. The redundant supervisor engine ROMMON upgrade process described next only works when the active supervisor engine is running Cisco IOS Release 15.0(2)SG. For redundant systems, you first upgrade the software to Cisco IOS Release 15.0(2)SG, then upgrade the ROMMON.

Upgrading the Supervisor Engine ROMMON from the Console

Caution To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

Note The examples in this section use the programmable read-only memory (PROM) upgrade version 12.2(44r)SG9 and Cisco IOS Release 12.2(50)SG. For other software releases, replace the ROMMON release and Cisco IOS software release with the appropriate release and filename. This document describes the procedure for a single supervisor engine system. In a dual supervisor engine system, you must perform the process on each supervisor engine.

Follow this procedure to upgrade your supervisor engine ROMMON:

Step 1 Directly connect a serial cable to the console port of the supervisor engine.

Note This section assumes that the console baud rate is set to 9600 (default). If you want to use a different baud rate, change the configuration register value for your switch.

Step 2 Download the cat4500-e-ios-promupgrade-122_44r_SG9 program from Cisco.com, and place it on a TFTP server in a directory that is accessible from the switch to be upgraded.

The cat4500-e-ios-promupgrade-122_44r_SG9 program is available on Cisco.com at the same location from which Catalyst 4500 system images are downloaded.

Step 3 Use the **dir bootflash:** command to ensure that sufficient space exists in Flash memory to store the PROM upgrade image. If you are using a CompactFlash card, replace **bootflash:** with **slot0:**

Note Because of CSCsu36751, you should use bootflash for this upgrade if your current ROMMON version is prior to 12.2(44r)SG3. Else, you might need to reseat the compact flash after rebooting.

Step 4 Download the cat4500-e-ios-promupgrade-122_44r_SG9 program into Flash memory using the **copy tftp** command.

The following example shows how to download the PROM upgrade image cat4500-e-ios-promupgrade-122_44r_SG9 from the remote host 172.20.58.78 to bootflash:

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4500-e-ios-promupgrade-122_44r_SG9]?
Destination filename [cat4500-e-ios-promupgrade-122_44r_SG9]?
Accessing tftp://172.20.58.78/cat4500-e-ios-promupgrade-122_44r_SG9...
Loading cat4500-e-ios-promupgrade-122_44r_SG9 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
[OK - 2404172 bytes]

2404172 bytes copied in 28.536 secs (84250 bytes/sec)
Switch#
```

Step 5 On a dual-supervisor system, copy the same ROMMON image to the standby supervisor engine with the **copy bootflash:cat4500-e-ios-promupgrade-122_44r_SG9 slavebootflash** command

Step 6 Enter the **reload** command to reset the switch, press **Ctrl-C** to stop the boot process, and re-enter ROMMON.

Note On a redundant system, this action causes a switchover.

The following example shows the output after a reset into ROMMON:

```
Switch# reload
Proceed with reload? [confirm]

03:57:16:%SYS-5-RELOAD:Reload requested ?


 Rom Monitor Program Version 12.2(44r)SG3


.
.(output truncated)
.

 Established physical link 1Gb Full Duplex
 Network layer connectivity may take a few seconds
rommon 1 >
```

Step 7 Run the PROM upgrade program by entering this command:
boot bootflash:cat4500-e-ios-promupgrade-122_44r_SG9

Caution No intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the process. Do not perform a reset, power cycle, or OIR of the supervisor engine until the upgrade completes.

The following example shows the output from a successful upgrade, followed by a system reset:

```
rommon 2 > boot bootflash:cat4500-e-ios-promupgrade-122_44r_SG9

Image Name : Cat4K_Mpc8548_Rommon
 Image size : 1048576 bytes
 Uncompressing image.....
 Done!

 **********************************************************
 *        ** Now Upgrading Primary ROMMON Image **        *
 **********************************************************

 Offset: 7E00000
erasing... writing... reading... verifying...  Done!


 **********************************************************
 *            ** Now Programming FPGA Image **            *
 **********************************************************

 Image Name : Cat4K_JAWA_Fpga
 Image size : 524288 bytes

 Uncompressing image.....
 Done!

Device ID 12, status  0, size 524288 bytes, we have 524288 bytes
erasing... writing/verifying sectors... 0 1 2 3 4 5 6 7 Done!
 **********************************************************
 System will now reset itself and reboot within few seconds
 **********************************************************
*!*

 **********************************************************
 *                                                        *
 * Welcome to Rom Monitor for WS-X45-SUP6-E System.       *
 * Copyright (c) 2003-2010 by Cisco Systems, Inc.         *
 * All rights reserved.                                   *
 *                                                        *
 **********************************************************
….
Rom Monitor Program Version 12.2(44r)SG9
 CPU Rev: 2.0, Board Rev: 4, Board Type: 10, CPLD Jawa Rev: 20
…
rommon 1>
```

Step 8 Boot the Cisco IOS software image. This may happen automatically if the system is configured to auto-boot.

Step 9 On a redundant system, hook up a console to the now-active supervisor engine. After the system achieves an SSO state, repeat steps 6-8.

Step 10 Use the **show module** command to verify that you have upgraded the ROMMON:

```
Switch# show module
Chassis Type : WS-C4510R-E

Power consumed by backplane : 40 Watts

Mod Ports Card Type                              Model              Serial No.
---+-----+--------------------------------------+------------------+-----------
 3    48  10/100/1000BaseT POE E Series          WS-X4648-RJ45V-E   JAE1129QL9N
 4    48  10/100/1000BaseT Premium POE E Series  WS-X4648-RJ45V+E   JAE1129QSAV
 5     6  Sup 6-E 10GE (X2), 1000BaseX (SFP)     WS-X45-SUP6-E      JAE1225MJMN
 6     6  Sup 6-E 10GE (X2), 1000BaseX (SFP)     WS-X45-SUP6-E      JAE1224LAOS
 7    48  10/100/1000BaseT (RJ45)V, Cisco/IEEE   WS-X4548-RJ45V+    JAB1229BCMD
 8    24  10/100/1000BaseT (RJ45)V, Cisco/IEEE   WS-X4524-GB-RJ45V  JAB0815059Q
```

```
M MAC addresses                    Hw  Fw           Sw               Status
--+--------------------------------+---+------------+----------------+---------
 3 001c.58f8.2240 to 001c.58f8.226f 0.3                               Ok
 4 001c.58f8.2090 to 001c.58f8.20bf 0.3                               Ok
 5 0017.94c9.85c0 to 0017.94c9.85c5 1.1 12.2(44r)SG9  12.2(50)SG      Ok
 6 0017.94c9.85c6 to 0017.94c9.85cb 1.1 12.2(44r)SG9  12.2(50)SG      Ok
 7 000a.8aff.3830 to 000a.8aff.385f 0.1                               Ok
 8 0030.850e.3e78 to 0030.850e.3e8f 0.6                               Ok   ….
Switch#
```

Step 11 Use the **delete** command on the active supervisor to delete the PROM upgrade program from bootflash

The following example shows how to delete the cat4500-e-ios-promupgrade-122_44r_SG9 image from bootflash:

```
Switch# delete bootflash:cat4500-e-ios-promupgrade-122_44r_SG9
```

Step 12 On a redundant system, also delete the upgrade file from the standby supervisor engine:

```
Switch# delete slavebootflash:cat4500-e-ios-promupgrade-122_44r_SG9
```

The ROMMON has now been upgraded.

See the "Upgrading the Cisco IOS Software" section on page 36 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Supervisor Engine ROMMON Remotely Using Telnet

Caution To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

Follow this procedure to upgrade your supervisor engine ROMMON to Release 12.2(44r)SG9. This procedure can be used when console access is not available and when the ROMMON upgrade must be performed remotely.

Note In the following section, use the PROM upgrade version bootflash:cat4500-e-ios-promupgrade-122_44r_SG9.

Step 1 Establish a Telnet session to the supervisor engine.

Note In the following discussion, we assume that at least one IP address has been assigned to either an SVI or a routed port.

Step 2 Download the bootflash:cat4500-e-ios-promupgrade-122_44r_SG9 program from Cisco.com, and place it on a TFTP server in a directory that is accessible from the switch to be upgraded.

The bootflash:cat4500-e-ios-promupgrade-122_44r_SG9 programs are available on Cisco.com at the same location from which you download Catalyst 4500 system images.

Step 3 Use the **dir bootflash:** command to ensure that there is sufficient space in Flash memory to store the PROM upgrade image. If there is insufficient space, delete one or more images, and then enter the **squeeze bootflash:** command to reclaim the space.

If you are using a CompactFlash card, replace **bootflash:** with **slot0:**.

Step 4 Download the bootflash:cat4500-e-ios-promupgrade-122_44r_SG9 program into Flash memory using the **copy tftp** command.

The following example shows how to download the PROM upgrade image bootflash:cat4500-e-ios-promupgrade-122_44r_SG9 from the remote host 172.20.58.78 to bootflash:

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [bootflash:cat4500-e-ios-promupgrade-122_44r_SG9]?
Destination filename [bootflash:cat4500-e-ios-promupgrade-122_44r_SG9]?
Accessing tftp://172.20.58.78/ bootflash:cat4500-e-ios-promupgrade-122_44r_SG9...
Loading bootflash:cat4500-e-ios-promupgrade-122_44r_SG9 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
[OK - 455620 bytes]

455620 bytes copied in 2.644 secs (172322 bytes/sec)
Switch#
```

Step 5 Use the **no boot system flash bootflash:***file_name* command to clear all BOOT variable commands in the configuration file. In this example, the BOOT variable was set to boot the image cat4000-i5s-mz.121-19.EW1.bin from bootflash:

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-i5s-mz.121-19.EW1.bin
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#

Use the boot system flash bootflash:file_name command to set the BOOT variable. You will
use two BOOT commands: one to upgrade the ROMMON and a second to load the Cisco IOS
software image after the ROMMON upgrade is complete. Notice the order of the BOOT
variables in the example below. At bootup the first BOOT variable command upgrades the
ROMMON. When the upgrade is complete the supervisor engine will autoboot, and the second
BOOT variable command will load the Cisco IOS software image specified by the second BOOT
command
```

Note The **config-register** must be set to autoboot.

```
In this example, we assume that the console port baud rate is set to 9600 bps and that the
config-register is set to 0x0102.

Use the config-register command to autoboot using image(s) specified by the BOOT variable.
Configure the BOOT variable to upgrade the ROMMON and then autoboot the IOS image after
the ROMMON upgrade is complete. In this example, we are upgrading the ROMMON to version
12.2(44r)SG9. After the ROMMON upgrade is complete, the supervisor engine will boot Cisco
IOS software Release 15.0(2)SG.

config-register to 0x0102.

Switch# configure terminal
Switch(config)# boot system flash bootflash:
bootflash:cat4500-e-ios-promupgrade-122_44r_SG9
Switch(config)# boot system flash bootflash:cat4500e-entservices-mz.1550-1.SG
Switch(config)# config-register 0x0102
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
```

```
Switch#
```

Step 6 Use the **show bootvar** command to verify the boot string. The BOOT variable in this example will first run the PROM upgrade to upgrade ROMMON. Then, the upgrade software will reload and the supervisor engine will load the Cisco IOS software image.

```
Switch# show bootvar
BOOT variable = bootflash:cat4000-ios-promupgrade-121_20r_EW1,1;bootflash:cat400
0-i9s-mz.121-20.EW1,1
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
```

Step 7 Run the PROM upgrade program by issuing the **reload** command. Issuing this command will terminate your Telnet session.

Caution Verify the boot string in step 6. No intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the upgrade process. Do not perform a reset, power cycle, or OIR of the supervisor engine until the upgrade is complete.

The following example shows the console port output from a successful ROMMON upgrade followed by a system reset. Your Telnet session is disconnected during the ROMMON upgrade, so you will not see this output. This step could take 2-3 minutes to complete. You will need to reconnect your Telnet session after 2-3 minutes when the Cisco IOS software image and the interfaces are loaded.

```
Switch# reload
Proceed with reload? [confirm]

1d05h: %SYS-5-RELOAD: Reload requested




 **********************************************************
 *                                                        *
 * Welcome to Rom Monitor for WS-X4515 System.            *
 * Copyright (c) 2002 by Cisco Systems, Inc.              *
 * All rights reserved.                                   *
 *                                                        *
 **********************************************************

 Rom Monitor Program Version 12.1(12r)EW

 Board type 2, Board revision 7
 Swamp FPGA revision 28, Dagobah FPGA revision 86

***** The system will autoboot in 5 seconds *****


 Type control-C to prevent autobooting.
 . . . . .
 Established physical link 100MB Full Duplex
 Network layer connectivity may take a few seconds


 ******** The system will autoboot now ********


 config-register = 0x0102
 Autobooting using BOOT variable specified file.....
 Current BOOT file is --- bootflash:cat4000-ios-promupgrade-121_20r_EW1



 ***********************************************************
 *                                                         *
 * Rom Monitor Upgrade Utility For  WS-X4515 System        *
 * This upgrades flash Rom Monitor image to the latest     *
 *                                                         *
 * Copyright (c) 2002, 2003 by Cisco Systems, Inc.         *
 * All rights reserved.                                    *
 *                                                         *
 ***********************************************************

 Image size = 314.236 KBytes

 Maximum allowed size = 511.75 KBytes


 Upgrading your PROM... DO NOT RESET the system
 unless instructed or upgrade of PROM will fail !!!

 Beginning erase of 0x80000 bytes at offset 0x3f80000...  Done!

 Beginning write of prom  (0x4e8ec bytes at offset 0x3f80000)...

 This could take as little as 30 seconds or up to 2 minutes.
 Please DO NOT RESET!

 Success! The prom has been upgraded successfully.
 System will reset itself and reboot in about 15
.
.(output truncated)
.
******** The system will autoboot now ********


 config-register = 0x0102
 Autobooting using BOOT variable specified file.....

 Current BOOT file is --- bootflash:cat4000-i9s-mz.121-20.EW1

Rommon reg: 0x56000380

Running IOS...

Decompressing the image
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
#################################################################### [OK]
```

Step 8 Use the **no boot system flash bootflash:***file_name* command to clear the BOOT command used to upgrade the ROMMON.

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
```

```
Switch#
```

Step 9 Use the **show version** command to verify that the ROMMON has been upgraded.

```
Switch# show version
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I9S-M), Version 12.1(20)EW, E
ARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 22-Oct-03 23:42 by kellmill
Image text-base: 0x00000000, data-base: 0x00F56DDC

ROM: 12.1(20r)EW1
Dagobah Revision 86, Swamp Revision 28

Switch uptime is 0 day, 0 hour, 5 minutes
System returned to ROM by reload
System image file is "bootflash:cat4000-i9s-mz.121-20.EW1"

cisco WS-C4503 (XPC8245) processor (revision 7) with 524288K bytes of memory.
Processor board ID FOX06460YD8
Last reset from Reload
3 Ethernet/IEEE 802.3 interface(s)
51 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
403K bytes of non-volatile configuration memory.

Configuration register is 0x0102

Switch#
```

Step 10 Use the **delete** command to delete the PROM upgrade program from bootflash and the **squeeze** command to reclaim unused space.

The following example shows how to delete the cat4000-ios-promupgrade-121_20r_EW1 image from bootflash and reclaim unused space:

```
Switch# delete bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch# squeeze bootflash:

All deleted files will be removed, proceed (y/n) [n]? y

Squeeze operation may take some time, proceed (y/n) [n]? y
Switch#
```

Step 11 Use the **show bootvar** command to verify that the ROMMON upgrade program has been removed from the BOOT variable.

```
Switch# show bootvar
BOOT variable = bootflash:cat4000-i9s-mz.121-20.EW1,1
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x0102
```

The ROMMON has now been upgraded.

See the "Upgrading the Cisco IOS Software" section on page 36 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Cisco IOS Software

Caution To avoid actions that might make your system unable to boot, please read this entire section before starting the upgrade.

Before you proceed, observe the following rules for hostname:

- Do not expect case to be preserved

  Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, Choosing a Name for Your Computer.
- Must start with a letter and end with a letter or digit.
- Interior characters can only be letters, digits, and hyphens; periods and underscores not allowed.
- Names must be 63 characters or fewer; hostname of fewer than 10 characters is recommended.
- On most systems, a field of 30 characters is used for the host name and the prompt in the CLI. Longer configuration mode prompts may be truncated.

To upgrade the Cisco IOS software on your Catalyst 4500 series switch, use this procedure:

Step 1 Download Cisco IOS Release 15.01(2) from Cisco.com, and place the image on a TFTP server in a directory that is accessible from the supervisor engine that is upgraded.

Step 2 Use the **dir bootflash:** command to ensure that there is sufficient space in Flash memory to store the **promupgrade** image. If there is insufficient space, delete one or more images, and then enter the **squeeze bootflash:** command to reclaim the space.

If you are using a CompactFlash card, use **slot0:** instead of **bootflash**.

Step 3 Download the software image into Flash memory using the **copy tftp** command.

The following example shows how to download the Cisco IOS software image cat4000-is-mz.121-12c.EW from the remote host 172.20.58.78 to bootflash:

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4000-is-mz121_12c.EW]?
Destination filename [cat4000-is-mz.121-12c.EW]?
Accessing tftp://172.20.58.78/cat4000-is-mz.121-12c.EW...
Loading cat4000-is-mz.121-12c.EW from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
|!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
[OK - 6923388/13846528 bytes]

6923388 bytes copied in 72.200 secs (96158 bytes/sec)
Switch#
```

Step 4 Use the **no boot system flash bootflash:***file_name* command to clear the cat4000-is-mz.121-8a.EW file and to save the BOOT variable.

The following example shows how to clear the BOOT variable:

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-is-mz.121-8a.EW
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

Step 5 Use the **boot system flash** command to add the Cisco IOS software image to the BOOT variable.

The following example shows how to add the cat4000-is-mz.121-12c.EW image to the BOOT variable:

```
Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4000-is-mz.121-12c.EW
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

Step 6 Use the **config-register** command to set the configuration register to 0x2102.

The following example show how to set the second least significant bit in the configuration register:

```
Switch# configure terminal
Switch(config)# config-register 0x2102
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3723 to 1312 bytes [OK]
Switch#
```

Step 7 Enter the **reload** command to reset the switch and load the software.

Caution CautionNo intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the upgrade process by performing a reset, power cycle, or OIR of the supervisor, for at least five minutes.

The following example shows the output from a successful upgrade followed by a system reset:

```
Switch# reload
Rommon reg: 0x2B004180

Upgrading FPGA...

Decompressing the image
############## [OK]

 *******************************************************
 *                                                     *
 * WS-X4014 FPGA Upgrade Utility For WS-X4014 Machines *
 *                                                     *
 * Copyright (c) 2002 by Cisco Systems, Inc.           *
 * All rights reserved.                                   *
 *                                                        *
 **********************************************************

 Image size = 483.944 KBytes

 Maximum allowed size = 1023.75 KBytes


 Upgrading your FPGA image... DO NOT RESET the system
 unless instructed or upgrade of FPGA will fail !!!

 Beginning erase of 0x100000 bytes at offset 0x3d00000...  Done!

 Beginning write of fpga image  (0x78fb0 bytes at offset 0x3d00000)...

 This could take as little as 30 seconds or up to 2 minutes.
 Please DO NOT RESET!

 Success! FPGA image has been upgraded successfully.
 System will reset itself and reboot in about 15 seconds.
 0




 **********************************************************
 *                                                        *
 * Welcome to Rom Monitor for WS-X4014 System.            *
 * Copyright (c) 2002 by Cisco Systems, Inc.              *
 * All rights reserved.                                   *
 *                                                        *
 **********************************************************

 Rom Monitor Program Version 12.1(12r)EW

 Board type 1, Board revision 5
 Swamp FPGA revision 16, Dagobah FPGA revision 47


 MAC Address  : 00-30-85-XX-XX-XX
 IP Address   : 10.10.10.91
 Netmask      : 255.255.255.0
 Gateway      : 10.10.10.1
 TftpServer   : Not set.
 Main Memory  : 256 MBytes

 ***** The system will autoboot in 5 seconds *****


 Type control-C to prevent autobooting.
Switch#
```

Step 8 Use the **show version** command to verify that the new Cisco IOS release is operating on the switch.

Limitations and Restrictions

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

All Supervisor Engines

- When you enter the **permit any any ?** command you will observe the **octal** option, which is unsupported in Cisco IOS Release 12.2(54)SG.

  CSCsy31324
- A Span destination of fa1 is not supported.
- The "keepalive" CLI is not supported in interface mode on the switch, although it will appear in the running configuration. This behavious has no impact on functionality.
- TDR is only supported on interfaces Gi1/1 through Gi1/48, at 1000BaseT under open or shorted cable conditions. TDR length resolution is +/- 10 m. If the cable is less than 10 m or if the cable is properly terminated, the TDR result displays "0" m. If the interface speed is not 1000BaseT, an "unsupported" result status displays. TDR results will be unreliable for cables extended with the use of jack panels or patch panels.
- The following guidelines apply to Fast UDLD:
  - Fast UDLD is disabled by default.
  - Configure fast UDLD only on point-to-point links between network devices that support fast UDLD.
  - You can configure fast UDLD in either normal or aggressive mode.
  - Do not enter the link debounce command on fast UDLD ports.
  - Configure fast UDLD on at least two links between each connected network device. This reduces the likelihood of fast UDLD incorrectly error disabling a link due to false positives.
  - Fast UDLD does not report a unidirectional link if the same error occurs simultaneously on more than one link to the same neighbor device.
- 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>
```

- Although the Catalyst 4500 series switch still supports legacy 802.1X commands used in Cisco IOS Release 12.2(46)SG and earlier releases (that is, they are accepted on the CLI), they do not display in the CLI help menu.
- Current IOS software cannot support filenames exceeding 64 characters.
- All software releases support a maximum of 32,768 IGMP snooping group entries.
- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

  This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

	QueueID	Old QueueName	New QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<unused queue>	control-packet
	11	<unused queue>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- 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 AC15624100000670001BC9.
```

  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

- For any configuration where the source-interface keyword is used, if you provide an SVI that is associated with a secondary private VLAN, configuration involving the secondary VLAN may be lost when the switch is reloaded. In such scenarios, always use the primary private VLAN.

For Supervisor Engines II+Plus through V-10GE

- For the IP Unnumbered feature, the following are not supported:
  - Dynamic routing protocols
  - HSRP/VRRP
  - Static ARP
  - Unnumbered interface and numbered interface in different VRFs
- For WCCP version 2, the following are not supported:
  - GRE encapsulation forwarding method
  - Hash bucket based assignment method
  - Redirection on an egress interface (redirection out)
  - Redirect-list ACL
- For IPX software routing, the following are not supported:
  - NHRP (Next Hop Resolution Protocol)
  - NLSP
  - Jumbo Frames
- For AppleTalk software routing, the following are not supported:
  - AURP
  - AppleTalk Control Protocol for PPP
  - Jumbo Frames
  - EIGRP
- For the Netflow feature, the following limitations apply:
  - Netflow will not account for control packets, packets that encountered link-level errors, and ARP/RARP packets.
  - The software cache for Netflow is fixed, users cannot change the size.
  - The statistical distribution row that displays the distribution across various packet sizes is not available.
- For the PBR feature, the following limitations apply:
  - Packet length-based matching policies are not supported.
  - IP Precedence, TOS and Qos groups are fixed.
  - ACL/Route-map statistics are not updated.
- IGRP is not supported (use EIGRP instead).
- The MAC address table is cleared when you switch between supervisor engines if either the 802.1s or 802.1w Spanning Tree Protocol is configured. To minimize address clearing and subsequent packet flooding, configure the edge ports as **spanning-tree portfast** and the link type as **spanning-tree link-type point-to-point**.

- While running NSF and IS-IS IETF mode, if you enter the **issu runversion** command within 5 minutes of entering the **issu loadversion** command, packet loss may occur during an ISSU upgrade.

  Workaround: Configure the NSF interval timer to 0 minutes, or delay entering the **issu runversion** command until the NSF interval timer expires and NSF restarts.

- Routes may not be properly redistributed from one routing protocol to another when NSF is enabled on the switch. The success of the redistribution depends on the order in which the routing protocols converge after an NSF switchover.

  Workaround: None.

- IP classful routing is not supported; do not use the **no ip classless** command; it will have no effect because only classless routing is supported. The **ip classless** command is not supported because classless routing is enabled by default.
- The Catalyst 4510R switch does not support Supervisor Engines II-Plus, III, IV, and II-Plus-10GE. Installing an unsupported supervisor engine causes unpredictable hardware behavior that cannot be controlled by the software. Using an unsupported supervisor engine in a redundant slot might cause a supported supervisor engine in the other slot to malfunction.
- Supervisor Engine II-Plus cannot read a CompactFlash card formatted by Supervisor Engine III or Supervisor Engine IV in a prior release.
- Catalyst 4500 supervisor engines will not be properly initialized if the VLAN configuration in the startup file does not match the information stored in the VLAN database file. This situation might occur if a backup configuration file was used.
- A Layer 2 LACP channel cannot be configured with the spanning tree PortFast feature.
- Netbooting using a boot loader image is not supported. See the "Troubleshooting" section on page 125 for alternatives.
- You cannot downgrade to Cisco IOS Release 12.1(8a)EW1 after running Release 12.1(13)EW (or higher). If you need to downgrade, contact your TAC representative for further instructions, and mention caveat CSCdz59058.
- Observe the following standard Cisco IOS software behavior when deploying redundant supervisor engines in a Catalyst 4507R chassis: While the startup configuration file is being parsed, the configuration file is not applied to hardware that does not exist.

  For example, if the active supervisor engine is in slot 1, and you have configured interface Gi1/1, the supervisor engine in slot 2 becomes active if you remove the active supervisor engine from the chassis. In addition, while the startup configuration file is being parsed, you will receive an error message indicating that interface Gi1/1 is no longer present. This behavior is correct. When the formerly active supervisor engine is reinserted into slot 1, there is no configuration for interface Gi1/1.

  This situation does not occur when both supervisor engines are present in the chassis.

  Workaround: Copy the startup configuration file into the running configuration:

  ```
  Switch# copy startup-config running-config
  ```

- An unsupported default CLI for mobile IP is displayed in the HSRP configuration. Although this CLI will not damage your system, you might want to remove it to avoid confusion.

  Workaround: Display the configuration with the **show standby** command, then remove the CLI. Here is an example of the **show standby GigabitEthernet1/1** command output:

  ```
  switch(config)# interface g1/1
  switch(config)# no standby 0 name (0 is hsrp group number)
  ```

- For HSRP preempt delay to function consistently, you must use the **standby delay minimum** command. Be sure to set the delay to more than 1 hello interval, which ensures that a hello is received before HSRP leaves the initiate state.

  Use the **standby delay reload** option if the router is rebooting after reloading the image.

- When you attempt to run OSPF between a Cisco router and a third-party router, the two interfaces might get stuck in the Exstart/Exchange state. This problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces do not match. If the router with the higher MTU sends a packet larger than the MTU set on the neighboring router, the neighboring router ignores the packet.

  Workaround: Because the problem is caused by mismatched MTUs, you should change the MTU on either router to match the other's MTU.

- You can run .1q-in-.1q packet passthrough with a Supervisor Engine III and a Supervisor Engine IV, but you can run only .1q-in-.1q encapsulation with a Supervisor Engine II+10GE, Supervisor Engine V, and Supervisor Engine V-10GE.
- For PVST and Catalyst 4500 E-Series switch VLAN, Cisco IOS Release 12.1(13)EW supports a maximum of 3000 spanning tree port instances. If you want to use more instances, use MST rather than PVST.
- Only ports 1 and 2 on the WS-X4418-GB module and ports 13 and 14 on the WS-X4412-2GB-T module can be set as ISL trunks.
- If an original packet is dropped due to transmit queue shaping or sharing configurations, a SPAN packet copy can still be transmitted on the SPAN port.
- For all software releases, do not use over 100,000 routes.
- Use the **no ip unreachables** command on all interfaces with ACLs configured for performance reasons.
- Layer 3 path load-balancing metrics are not supported in Cisco IOS Releases 12.1(8a)EW, 12.1(11b)EW, 12.1(12c)EW, 12.1(13)EW, 12.1(19)EW, and 12.1(20)EW. (CSCdv10578)
- The threshold for the Dynamic ARP Inspection err-disable function is set to 15 ARP packets per second per interface. You should adjust this threshold depending on the network configuration. The CPU should not receive DHCP packets at a sustained rate greater than 1000 pps.
- A limited number of ACL bindings are dynamically installed by the IP source guard feature on a Catalyst 4500 series switch Supervisor Engine II-Plus. To take full advantage of the IP source guard feature, you should use Supervisor Engine IV.
- If you first configure an IP address or IPv6 address on a Layer 3 port, then change the Layer 3 port to a Layer 2 port with the **switchport** command, and finally change it back to a Layer 3 port, the original IP/IPv6 address is lost.
- By default, IPv6 is not enabled. To route IPv6, you must enter the **IPv6 unicast-routing** command. If you plan to use IPv6 multicast routing, use the **IPv6 multicast-routing** command.
- By default, CEF is not enabled for IPv6 (after IPv6 unicast routing is enabled). To prevent IPv6 traffic from being process-switched, use the **IPv6 cef** command.
- Multicast sources in community VLANs are not supported.
- Two-way community VLANs are not supported.
- Voice VLANs are not supported on community VLAN host interfaces.
- Private VLAN trunks do not carry community VLANs.
- When you use private VLANs on the WS-4516 module, old ARP entries will not tim eout of the ARP cache if you do not manually clear the entry. This event has no affect on production.

- Compact flash formatted in Cisco IOS Release 12.2(20)EW should be reformatted in Release 12.2(25)EW on both Supervisor Engine V-10GE and non-Supervisor V-10GE systems. Compact flash formatted on any other release does not need to be reformatted on non-Supervisor Engine V-10GE systems.
- In a redundant system, do not remove and reinsert the standby supervisor engine while the active supervisor engine is booting up. Doing so may cause a failure in the online diagnostics test.

  Workaround: Remove and reinsert the standby supervisor engine after the active supervisor engine boots. (CSCsa66509)
- When used in conjunction with a 10-slot chassis, Supervisor Engine V only supports the Catalyst 4500 series two-port Gigabit Ethernet line card (WS-X4302-GB) in the 10th slot.
- The maximum number of unique private VLAN pairs supported by the **switchport private-vlan mapping trunk** command is 500. For example, one thousand secondary VLANs could map to one primary VLAN, or one thousand secondary VLANs could map one to one to one thousand primary VLANs.
- Support for PoE depends on the use of line cards and power supplies that support PoE.

  PoE switching modules:
  - WS-X4148-RJ45V
  - WS-X4224-RJ45V
  - WS-X4248-RJ45V
  - WS-X4248-RJ21V
  - WS-X4524-GB-RJ45V
  - WS-X4548-GB-RJ45V
  - 'WS-X4548-GB-RJ45V+

  PoE-enabled power supplies:
  - PWR-C45-1300ACV
  - PWR-C45-1400DC
  - PWR-C4K-2800AC
  - PWR-C45-1400AC
  - PWR-C45-1300ACV
  - 'PWR-C45-6000ACV'
- The maximum number of mappings for configuring PVLAN promiscuous trunk ports is 500 primary VLANs to 500 secondary VLANs.
- The 802.1X inaccessible authentication bypass feature is not supported with the NAC LAN port IP feature.
- Changes to the console speed in line console 0 configuration mode do not affect console speed in ROMMON. To apply the same console speed in ROMMON, use the confreg ROMMON utility.
- Supervisor Engine II-Plus does not support compact flashes formatted by an Cisco IOS image prior to Cisco IOS Release 12.2(19)EW.
- If a Catalyst 4500 series switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to following appears:

```
00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not 
responding.
```

If this message appears, verify that the switch is connected to the ACS. You should also ensure that the switch has been properly configured as an AAA client on the ACS.

- The **bgp shutdown** command is not supported in BGP router configuration mode. Entering this command might produce unexpected results.
- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)
- Interfaces on the module WS-X4148-RJ45V may not establish a link with a Daiden DN-2800G media converter when both the switch and the media converter interfaces are configured to operate at 100 Mbps and full duplex. This situation occurs when the interface on the module is configured to automatically detect and power up devices inline with the **power inline auto** command. This caveat appears in all software releases.

  Workarounds:

  1. Disable inline power on the switch ports using the **power inline never** command.

  2. Configure the media converter to autonegotiate the speed and duplex instead of running them at 100 Mbps and full duplex. (CSCee62109)
- IPSG for static hosts supports the same port mode as IPSG except that it does not support trunk port:
  - It supports Layer 2 access port and PVLAN host port (isolated or community port).
  - It does not support trunk port, Layer 3 port, or EtherChannel.
- IPSG for static hosts should not be used on uplink ports.
- Selective DBL is only supported for non-tagged or single-tagged IP packets. To achieve Selective DBL-like functionality with a non-IP packet (like Q-in-Q and IPX), apply an input policy map that matches CoS values and specifies DBL in the class map.
- For Selective DBL, if the topology involves Layer 2 Q in Q tunneling, the match cos policy map will apply to the incoming port.
- If a set of DSCP values are already configured (for example, 0-30, 0-63), specifying a subset of these DSCP values with the **qos dbl dscp-based 0-7** command will not remove the unwanted DSCP values of 8 through 63. You must use the **no** form of the command to remove the extraneous values. In this case, the **no qos dbl dscp-based 8-63** command will leave 0-7 selected.
- When you use Port Security with Multi Domain Authentication (MDA) on an interface:
  - Allow for at least three MAC addresses to access the switch: two for the phone (the MAC address of a phone gets registered to the Data domain and Voice domain), and one for the PC.
  - Ensure that the data and voice VLAN IDs differ.
- For IP Port Security (IPSG) for static hosts, the following apply:
  - As IPSG learns the static hosts on each interface, the switch CPU may achieve 100 percent if there are a large number of hosts to learn. CPU usage will drop after the hosts are learned.
  - IPSG violations for static hosts are printed as they occur. If multiple violations occur simultaneously on different interfaces, the CLI displays the last violation. For example, if IPSG is configured for 10 ports and violations exist on ports 3, 6, and 9, the violation messages are printed only for port 9.
  - Inactive host bindings will appear in the device tracking table when either a VLAN is associated with another port or a port is removed from a VLAN. So, as hosts are moved across subnets, the hosts appear in the device tracking table as Inactive.

  - Autostate SVI does not work on EtherChannel.
- With the resolution of CSCsg08775, a GARP ACL entry is no longer part of the Static CAM area. However, a system-defined GARP class in Control Plane Policing (CPP) still exists.
- Certain configurations on the Catalyst 4507R and Catalyst 4510R chassis exceed the available maximum data power. These configurations include a combination of the follow PIDs:
  - Seven-slot configuration
  - Chassis WS-C4507R-E, WS-C4510R-E
  - Dual supervisor WS-X45-Sup6-E
  - One or more of the models WS-X4448-GB-RJ45 or WS-X4148-FX-MT

  To maximize the 10/100/1000 port density of 7- and 10-slot chassis when using redundant Supervisor Engine 6-E, install WS-X4548-GB-RJ45 instead of WS-X4448-GB-RJ45 line cards. If you require WS-X4448-GB-RJ45 line cards, two options are available:

  - Option 1

    Only four line card slots can be used on the Catalyst 4507R and six line card slots on the Catalyst 4510R chassis.
  - Option 2

    When all slots are required, only one model WS-X4448-GB-RJ45 line card can be used.

  To maximize the 100-BASE-FX port density of 7 and 10 slot chassis when using Supervisor Engine 6-E install WS-4248-FE-SFP line cards with FX optics instead of WS-X4148-FX-MT line cards. If WS-X4148-FX-MT line cards are required, two options are available:

  - Option 1

    You can use only 4 linecard slots on the Cat4507R chassis and 6 line card slots on the Cat4510R chassis.
  - Option 2

    When all slots are required, you can only use one WS-X4448-GB-RJ45 line card.
- When IPv6 is enabled on an interface through any CLI, you might see the following message:

  ```
  % Hardware MTU table exhausted
  ```

  In such a scenario, the IPv6 MTU value programmed in hardware differs from the IPv6 interface MTU value. This will happen if no room exists in the hardware MTU table to store additional values.

  To create room in the table, unconfigure some unused MTU values. Then, either disable or reenable IPv6 on the interface, or reapply the MTU configuration.
- To stop IPSG with static hosts on an interface, use the following commands in interface configuration submode:

  ```
  Switch(config-if)# no ip verify source
  Switch(config-if)# no ip device tracking max
  ```

  To enable IPSG with static hosts on a port, enter the following commands:

  ```
  Switch(config)# ip device tracking ****enable IP device tracking globally
  Switch(config)# ip device tracking max <n> ***set an IP device tracking maximum on int
  Switch(config-if)# ip verify source tracking [port-security] ****activate IPSG on port
  ```

Caution If you configure the **ip verify source tracking** [**port-security**] interface configuration command on a port without enabling IP device tracking globally or setting an IP device tracking maximum on that interface, IPSG with static hosts reject all the IP traffic from that interface.

Note The preceding condition also applies to IPSG with static hosts on a PVLAN host port.

- You must disable hardware control plane policing by removing the **system-cpp-policy** named ACL from the controlplane before performing an ISSU upgrade between Cisco IOS Release 12.2(40)SG and a previous release. You cannot detach **system-cpp-policy** named ACL from the controlplane in previous releases. If you are running a previous release, you must first upgrade to the latest maintenance release in the Cisco IOS Release 12.2(31) SGA*x* while performing an ISSU upgrade to Cisco IOS Release 12.2(40)SG.
- On a Supervisor Engine V-10GE (WS-X4516-10GE) in a 10-slot chassis (Catalyst 4510R and 4510RE), if a startup configuration with a new uplink mode is copied into flash memory and the system is power cycled, the system will not start with the new uplink mode. After you copy the startup configuration with the new uplink mode into flash memory, you must change the uplink mode to the new uplink mode through the command interface before the system is power cycled. This ensures that the system starts in the new uplink mode.
- When you use Supervisor Engine V in a Catalyst 4510R or 4510R-E chassis, slot 10 (FlexSlot) only supports the following linecards: the two-port GBIC (WS-X4302-GB) and the Access Gateway Module (WS-X4604-GWY). Supervisor Engine V-10GE has this same restriction when you configure its uplink select mode to **all**. Supervisor Engine V-10GE supports all Catalyst 4500 Series linecards in slot 10 when its uplink select mode is configured as tengigabitethernet or gigabitethernet. Supervisor Engine 6-E supports all Catalyst 4500 series linecards in slot 10.
- Prior to Cisco IOS Release 12.2(50)SG, on switches with Supervisor Engines V, V-10GE and earlier, class-map hit statistics on a user defined class-map in system-cpp-policy are not updated properly. With Cisco IOS Release 12.2(50)SG, the hit statistics for user-defined class-map in the system-cpp-policy are updated properly. However, in per-vlan capture mode, the hit stats for system defined in system-cpp-policy are not updated. In the global capture mode, hit stats for all class-maps (user-defined and system-defined) in the system-cpp-policy are updated properly.
- If you use MDA or multi-auth host mode in conjunction with pre-authentication open access, a switch ignores unicast EAPOL responses.

  Workarounds:

  – Force the supplicant to use multicast EAPOL.

  – Avoid authentication open mode. CSCtq33048

For Supervisor Engine 6-E and Supervisor Engine 6L-E

- The Catalyst 4510R switch does not support Supervisor Engines 6L-E. Installing an unsupported supervisor engine causes unpredictable hardware behavior that cannot be controlled by the software. Using an unsupported supervisor engine in a redundant slot might cause a supported supervisor engine in the other slot to malfunction.

- The MAC address table is cleared while you switch between supervisor engines if either the 802.1s or 802.1w Spanning Tree Protocol is configured. To minimize address clearing and subsequent packet flooding, configure the edge ports as **spanning-tree portfast** and the link type as **spanning-tree link-type point-to-point**.
- IP classful routing is not supported; do not use the **no ip classless** command; it will have no effect, because only classless routing is supported. The command **ip classless** is not supported because classless routing is enabled by default.
- A Layer 2 LACP channel cannot be configured with the spanning tree PortFast feature.
- Netbooting using a boot loader image is not supported. See the "Troubleshooting" section on page 125 for alternatives.
- When you deploy redundant supervisors in a Catalyst 4507R, for hardware that does not exist while the startup configuration file is being parsed, the configuration file for the hardware is not applied.

  For example, if the active supervisor engine is in slot 1, and you have configured interface Gi1/1, the supervisor engine in slot 2 becomes active if you remove the active supervisor engine from the chassis. In addition, while the startup configuration file is being parsed, you will receive an error message indicating that interface Gi1/1 is no longer present. This behavior is correct. When the formerly active supervisor engine is reinserted into slot 1, there is no configuration for interface Gi1/1.

  This situation will not occur when both supervisor engines are physically in the chassis.

  Workaround: Copy the startup configuration file into the running configuration:

  ```
  Switch# copy startup-config running-config
  ```

- An unsupported default CLI for mobile IP is displayed in the HSRP configuration. Although this CLI will not harm your system, you might want to remove it to avoid confusion.

  Workaround: Display the configuration with the **show standby** command, then remove the CLI. Here is an example of **show standby GigabitEthernet1/1** command output:

  ```
  switch(config)# interface g1/1
  switch(config)# no standby 0 name (0 is hsrp group number)
  ```

- For HSRP preempt delay to function consistently, you must use the **standby delay minimum** command. Be sure to set the delay to more than 1 hello interval, thereby ensuring that a hello is received before HSRP leaves the initiate state.

  Use the **standby delay reload** option if the router is rebooting after reloading the image.
- When you attempt to run OSPF between a Cisco router and a third party router, the two interfaces might get stuck in the Exstart/Exchange state. This problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces do not match. If the router with the higher MTU sends a packet larger than the MTU set on the neighboring router, the neighboring router ignores the packet.

  Workaround: Ensure that the MTUs match.
- You can run only .1q-in-.1q packet pass-through with Supervisor Engine 6-E.
- For PVST and Catalyst 4500 E-Series switch VLAN, Cisco IOS Release 12.1(13)EW support a maximum of 3000 spanning tree port instances. If you want to use more instances, use MST rather than PVST.
- Because the Supervisor Engine 6-E supports the FAT filesystem, the following restrictions apply:
  - The **verify** and **squeeze** commands are not supported.
  - The **rename** command is supported in FAT file system.

For Supervisor Engine 6-E, the **rename** command is available for bootflash and slot0. For all other supervisor engines, the **rename** command is supported for nvram devices only.

  - The **fsck** command is supported for slot0 device. It is not supported in the file systems on supervisor engines other than 6-E.
  - In the FAT file system, the IOS **format bootflash:** command erases user files only. It does not erase system configuration.
  - The FAT file system supports a maximum of 63 characters for file/directory name. The maximum for path length is 127 characters.
  - The FAT file system does not support the following characters in file/directory names:{ }#%^ and space characters.
  - The FAT file system honors the Microsoft Windows file attribute of read-only and read-write, but it does not support the Windows file hidden attribute.
  - Supervisor Engine 6-E uses the FAT file system for compact flash (slot0). If a compact flash is not formatted in FAT file system (such as compact flash on a supervisor engine other than 6-E), the switch does not recognize it.

- If an original packet is dropped because of transmit queue shaping or sharing configurations, a SPAN packet copy can still be transmitted on the SPAN port.
- All software releases support a maximum of 16,000 IGMP snooping group entries.
- To maximize performance, use the **no ip unreachables** command on all interfaces that are configured for ACLs.
- The threshold for the Dynamic Arp Inspection err-disable function is set to 15 ARP packets per second per interface. You should adjust this threshold depending on the network configuration. The CPU should not receive DHCP packets at a sustained rate greater than 1000 pps.
- If you first configure an IP address or IPv6 address on a Layer 3 port, then change the Layer 3 port to a Layer 2 port with the **switchport** command, and finally change it back to a Layer 3 port, the original IP/IPv6 address is lost.
- In a redundant system, do not remove and reinsert the standby supervisor engine while the active supervisor engine is booting. Doing so may cause the online diagnostics test to fail.

  Workaround: Remove and reinsert the standby supervisor engine after the active supervisor engine boots. (CSCsa66509)
- The **switchport private-vlan mapping trunk** command supports a maximum of 500 unique private VLAN pairs. For example, 500 secondary VLANs could map to one primary VLAN, or 500 secondary VLANs could map to 500 primary VLANs.
- Support for PoE depends on the use of the following line cards and power supplies.

  PoE switching modules:
  - WS-X4148-RJ45V
  - WS-X4224-RJ45V
  - WS-X4248-RJ45V
  - WS-X4248-RJ21V
  - WS-X4524-GB-RJ45V
  - WS-X4548-GB-RJ45V
  - WS-X4648-RJ45V-E
  - WS-X4648-RJ45V+E

  - WS-X4548-GB-RJ45V+

  PoE enabled power supplies:

  - PWR-C45-1300ACV
  - PWR-C45-1400DC
  - PWR-C4K-2800AC
  - PWR-C45-1400AC
  - PWR-C45-1300ACV
  - PWR-C45-6000ACV

- If a Catalyst 4500 series switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

  ```
  00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not
  responding.
  ```

  If this message appears, ensure network connectivity exists between the switch and the ACS. Also check that the switch has been properly configured as an AAA client on the ACS.

- For IP Port Security (IPSG) for static hosts, the following apply:
  - As IPSG learns the static hosts on each interface, the switch CPU may achieve 100 percent if there are a large number of hosts to learn. The CPU usage will drop after the hosts are learned.
  - IPSG violations for static hosts are printed as they occur. If multiple violations occur simultaneously on different interfaces, the CLI displays the last violation. For example, if IPSG is configured for 10 ports and violations exist on ports 3,6, and 9, the violation messages are printed only for port 9.
  - Inactive host bindings will appear in the device tracking table when either a VLAN is associated with another port or a port is removed from a VLAN. So, as hosts are moved across subnets, the hosts appear in the device tracking table as inactive.
  - Autostate SVI does not work on EtherChannel.

- When IPv6 is enabled on an interface with any CLI, you might see the following message:

  ```
  % Hardware MTU table exhausted
  ```

  In such a scenario, the IPv6 MTU value programmed in hardware differs from the IPv6 interface MTU value. This occurs if no room exists in the hardware MTU table to store additional values.

  To create room, unconfigure some unused MTU values. Then, either disable or re-enable IPv6 on the interface, or reapply the MTU configuration.

- To stop IPSG with static hosts on an interface, use the following commands in interface configuration submode:

  ```
  Switch(config-if)# no ip verify source
  Switch(config-if)# no ip device tracking max
  ```

  To enable IPSG with static hosts on a port, enter the following commands:

  ```
  Switch(config)# ip device tracking ****enable IP device tracking globally
  Switch(config)# ip device tracking max <n> ***set an IP device tracking maximum on int
  Switch(config-if)# ip verify source tracking [port-security] ****activate IPSG on port
  ```

Caution If you configure the **ip verify source tracking [port-security]** interface configuration command on a port without enabling IP device tracking globally or setting an IP device tracking maximum on that interface, IPSG with static hosts reject all the IP traffic from that interface.

Note The preceding condition also applies to IPSG with static hosts on a PVLAN host port.

- uRPF supports up to four paths. If a packet arrives at one of the valid VLANs that is not programmed as one of the RPF VLAN in hardware, it is dropped. If traffic may arrive from any other interfaces without RPF configured, it can be switched.
- Input and output ACLs cannot override or filter traffic received on an uRPF interface.
- No CLI command exists to reflect uRPF drop packets during hardware switching. The **sh ip traffic** and **show cef int** commands do not reflect uRPF drops.
- IPv6 ACL is not supported on a switchport. IPv6 packets cannot be filtered on switchports using any of the known methods: PACL, VACL, or MACLs.
- Class-map match statements using **match ip prec | dscp** match only IPv4 packets, whereas matches performed with **match prec | dscp** match both IPv4 and IPv6 packets.
- IPv6 QoS hardware switching is disabled if the policy-map contains IPv6 ACL and match CoS in the same class-map with the IPv6 access-list has any mask within the range /81 and /127. This situation causes forwarding packets to software, which efficiently disables the QoS.
- When the following data-only Catalyst 4500 linecards are used in a Catalyst 4507R-E or 4510R-E chassis with Supervisor Engine 6-Es, the capacity of the power supply may be exceeded:
  - WS-X4148-FX-MT Cisco Catalyst 4500 Fast Ethernet Switching Module, 48-port 100BASE-FX (MT-RJ)
  - WS-X4448-GB-RJ45 Cisco Catalyst 4500 48-port 10/100/1000 Module (RJ-45)

  The Catalyst 4503-E and Catalyst 4506-E have no caveats. The Catalyst 4507R-E configurations that use power supplies rated at 1400 W or above also have no caveats.

  The following replacement switching modules will not exceed the power supply capacity for any Catalyst 4500-E chassis:

	Recommended Replacement	Description
WS-X4148-FX-MT	WS-X4248-FE-SFP	Fast Ethernet, 48-port 100BASE-X (SFP)
WS-X4448-GB-RJ45	WS-X4548-GB-RJ45	Enhanced 48-port 10/100/1000 Module (RJ-45)
WS-X4448-GB-RJ45	WS-X4648-RJ45V-E	E-Series 48-port 802.3af PoE 10/100/1000 (RJ-45)

  Refer to the *Catalyst 4500 Series Module Installation Guide* to determine the power requirements for all of the Catalyst 4500 linecards and the power capacities of the Catalyst 4500 power supplies.

- Supervisor Engine 6-E *only* supports Catalyst 4500 Series linecards in slots 8-10.

- If you remove a line card from a redundant switch and initiate an SSO switch-over, then reinsert the line card, all interfaces are shutdown. The remaining configuration on the original line card is preserved.

  This situation only occurs if a switch reached SSO before you removed the line card.
- On Supervisor Engine 6-E, upstream ports support flow control auto negotiation in 1G mode only, and flow control is forced in 10G mode. If the interface is configured to auto-negotiate the flow control, and the interface is operating in 10G mode, the system forces flow control to ON and does not auto-negotiate.
- Supervisor Engine 6-E supports fast UDLD on a maximum of 32 ports.
- With Cisco IOS Release 12.2(53)SG3 (and 12.2(54)SG), we changed the default behavior such that your single supervisor, RPR, or fixed configuration switch does not reload automatically. To configure automatic reload, you must enter the **diagnostic fpga soft-error recover aggressive** command. (CSCth16953)

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 All caveats in Release 12.4 also apply to the corresponding 12.1 E releases. Refer to the *Caveats for Cisco IOS Release 12.4* publication at the following URL: http://www.cisco.com/en/US/docs/ios/12_4/release/notes/124MCAVS.html

Note For the latest information on PSIRTS, refer to the Security Advisories on CCO at the following URL: http://tools.cisco.com/security/center/publicationListing

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 Release 15.0(2)SG11

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

Table 10 Resolved Caveats in IOS Release 15.0(2)SG11

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
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 Release 15.0(2)SG10

- The Cisco IOS -XE software for 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

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing key pair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. CSCsb11964

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

  Workaround: None. CSCsg58526

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. CSCsg27395

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  Workaround: None. This is an informational message. CSCsi60898

- An IP unnumbered configuration is lost after a switch reloads.

  Workarounds: Do one of the following:

  – After a reload, copy the startup-config to the running-config.

  – Use a loopback interface as the target of the **ip unnumbered** command.

  – Change the CLI configuration so that during bootup the router port is created first.

  CSCsq63051

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. CSCsr00333

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

  Workaround: Configure an ISL/dot1q trunk port. CSCsu43445

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change. CSCsv44866

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

  Workaround: None. CSCsw14005

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

  If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine’s MAC address table, causing possible connectivity interruption on the host.

  Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

  This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

  Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

  The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

  CSCsz34522

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the |**auto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

  Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command. CSCta16492

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. CSCta61825

Workaround: None CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for a Catalyst 4900M switch, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Despite the different default value, you can configure any value in the time range.

  Workaround: None. CSCte51948
- On a peer interface on a Catalyst 4948E Ethernet Switch, if errdisabled mode flap detection is set to a very small number (such as 2 flaps in 10 sec), a 10GE link flap may cause the peer interface to enter the errdisabled state.

  Workarounds: The Cisco switch default link-flap detection value is 5 flaps in 10 seconds. Use the default value or larger numbers. CSCtg07677
- After you have enabled EPM logging and the client is authenticated via MAB or Webauth, the value of AUTHTYPE is DOT1X in EPM syslog messages irrespective of the authentication method.

  Similarly, the **show epm sessions** command always displays the authentication method as DOT1X.

  Workaround: To view the authentication method used for a client, enter the **show authentication sessions** command. CSCsx42157
- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

  Workaround: None. CSCso93282
- 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**, and then **no shut** on the ports. CSCtn88228
- 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 reboot a switch, the configured value of the interface MTU size on the members of the port channel interface does not function for IPv6 traffic.

  Workaround: After the switch reloads, enter **shut**, and 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

- When you have two Layer 3 CE-facing interfaces, each connected to a CE to split WCCP between the CEs, and you move a WCCP service (such as 60 (ftp-native)) from one interface to the other, the target interface fails to completely transfer the service from the old to the new CE.

  Workaround: Shut down the CE-facing interface. After all of the mask-value entries point to the target CE, unshut the CE-facing interface. CSCtl09941
- 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
- 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

Not Supported on Supervisor Engine 6-E

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  Workaround: None. (CSCso68331)

Supervisor Engine 6-E and Supervisor Engine 6L-E Specific Caveats

- Occasionally, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

  Workaround: Reinsert the X2. CSCsk43618
- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

  Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. CSCsi71036
- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

  Workaround: None.

  If you enter the **show policy**-**map** *name*, however, the unconditional marking actions appear. CSCsi94144
- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

  Workaround: None. CSCsl72868
- Uplinks go down when you upgrade the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

  This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine’s ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

  - Reload both supervisor engines with the **redundancy reload shelf** command.
  - Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

    There is *no* workaround for the link flap issue. CSCsm81875

- Changing the flow control configuration with traffic and pause frames causes some traffic loss.

  This problem can happen when pause frames are sent to a switch port and the flow control receive configuration is toggled on a 10-Gigabit Ethernet port.

  Workaround: Change the flow control receive configuration when no traffic exists. CSCso71647

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

  Workaround: None. CSCsq99468

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

  You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then later allocate the same VLAN.

  Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

  Workaround: Disable native VLAN tagging on the trunk port of the switch by entering the **no switchport trunk native vlan tag** command. CSCsz12611

- Before large PACLs are fully loaded in hardware, you might observe a false completion messages like the following:

  ```
  Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-HWPROGSUCCESS: Input Security: pacl - now
  fully loaded in hardware *Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All
  configured ACLs now fully loaded in hardware - hardware switching / QoS restored.
  ```

  Workaround: No functional impact.

  You must wait for the ACLs to be programmed before performing other TCAM related changes. CSCtd57063

- If a large number of VLAN mappings are configured, a member port might fail to join a port channel and no warming is issued.

  Workaround: Reduce the number of VLAN mappings. CSCtn56208

- WCCP service is not reacquired when a service group with a multicast group address is unconfigured, and then reconfigured.

  Workaround: Configure IP multicast routing globally and establish IP PIM sparse dense mode on the CE-facing interface. CSCtl97692

- If an interface whose IP address is being used as the router ID is deleted or shuts down, and you configure a service group with a multicast group address, packet redirection to CE stops and packets are forwarded directly to the destination.

  Workaround: Unconfigure and reconfigure the service group. CSCtn88087

- Global WCCP service configuration fails to enable (WCCP global configuration is accepted but nvgen fails) on a newly deployed switch if the switch is not enabled for SVI or a Layer 3 interface.

  Workaround: Enable a Layer 3 interface in the running configuration. CSCsc88636.

- 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

Resolved Caveats in Cisco IOS Release 15.0(2)SG10

- 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 Release 15.0(2)SG9

- 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 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 the *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 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.

  Workaround: mac-address-table limit is removed.

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 the *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 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 the *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

- Supervisor Engine 6-E may exhibit high CPU utilization in the output for these commands:
  - The **show process cpu** privileged EXEC command for 'Cat4k Mgmt LoPri'
  - The **show platform health** privileged EXEC command under KxAclPathMan update

  The increase is observed when configuring input and output service policies on trunk links that carry numerous VLANs, which, in turn, are enabled with other ACL based features (For examplem access-groups and PBR).

  Workaround: Reduce CPU utilization by removing unnecessary service policies from the trunk links. CSCui19835

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

  Workaround: Avoid custom pages. CSCui71349

- In PIM-DM mode, on a Cisco Catalyst 4948-E switch that is not the first hop router, the first mcast packet is dropped.

  Workaround: None. CSCul62120

- Removing a VLAN Mapping statement causes all traffic to be consistently dropped for other VLAN mapping statements.
  - 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 i**nterface 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 interfaces
2 Ten Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.

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

  Workaround: Reapply the configuration when the switch reboots. CSCum71764
- 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"
- If Supervisor Engine 2 running Cisco IOS Release 12.2(53)SG6 and a phone and PC are connected to a port in multi-auth mode with authentication open, and both devices are authenticated (or authorized) via MAB, after 30 seconds, both sessions are removed without any reason:

```
AUTH-FEAT-MDA-EVENT (Fa3/6): Deleting all clients in domain DATA
```

  Workaround: None. CSCuo56266
- 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

- 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

- 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

Resolved Caveats in Cisco IOS Release 15.0(2)SG8

This section lists the resolved caveats in Release 15.0(2)SG8:

- 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

- In the output of the **show interface** command, output counters for an EtherChannel member remain zero provided the ports are flapped from a peer and the switch is either Catalyst 4900M, Catalyst 4948E, or 4948E-F, or the supervisor engine is either 6E or 6L-E.

  Workaround: Enter the **show platform software interface Gix/xx statistic** command.

  CSCuf60629

Open Caveats for Cisco IOS Release 15.0(2)SG6

This section lists the open caveats for Cisco IOS Release 15.0(2)SG6:

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing key pair is used in the new certificate.

  On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

  Workaround: Reconnect. CSCsb11964

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

  Workaround: None. CSCsg58526

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. CSCsg27395

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  Workaround: None. This is an informational message. CSCsi60898

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

  - After a reload, copy the startup-config to the running-config.
  - Use a loopback interface as the target of the **ip unnumbered** command.
  - Change the CLI configuration so that during bootup the router port is created first.

  CSCsq63051

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

  Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. CSCsr00333

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

  Workaround: Configure an ISL/dot1q trunk port. CSCsu43445

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

  Workaround: Do one of the following:

  - Reload the standby switch again with the line card in place.
  - Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change. CSCsv44866

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  This applies to classic or E-series Catalyst 4500 supervisor engines running
  Cisco IOS Release 12.2(50)SG

  Workaround: None. CSCsw14005

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

  If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

  Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct. CSCsz20149

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

  This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

  Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

  The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

  CSCsz34522

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **auto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

  Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command. CSCta16492

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

  Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. CSCta61825

  Workaround: None CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for a Catalyst 4900M switch, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Despite the different default value, you can configure any value in the time range.

  Workaround: None. CSCte51948

- On a peer interface on a Catalyst 4948E Ethernet Switch, if errdisabled mode flap detection is set to a very small number (such as 2 flaps in 10 sec), a 10GE link flap may cause the peer interface to enter the errdisabled state.

  Workarounds: The Cisco switch default link-flap detection value is 5 flaps in 10 seconds. Use the default value or larger numbers. CSCtg07677

- After you have enabled EPM logging and the client is authenticated via MAB or Webauth, the value of AUTHTYPE is DOT1X in EPM syslog messages irrespective of the authentication method.

  Similarly, the **show epm sessions** command always displays the authentication method as DOT1X.

  Workaround: To view the authentication method used for a client, enter the **show authentication sessions** command. CSCsx42157

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

  Workaround: None. CSCso93282

- 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**, and then **no shut** on the ports. CSCtn88228
- 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
- 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 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
- When you have two Layer 3 CE-facing interfaces, each connected to a CE to split WCCP between the CEs, and you move a WCCP service (such as 60 (ftp-native)) from one interface to the other, the target interface fails to completely transfer the service from the old to the new CE.

  Workaround: Shut down the CE-facing interface. After all of the mask-value entries point to the target CE, unshut the CE-facing interface. CSCtl09941
- 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

Not Supported on Supervisor Engine 6-E

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  Workaround: None. (CSCso68331)

Supervisor Engine 6-E and Supervisor Engine 6L-E Specific Caveats

- Occasionally, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

  Workaround: Reinsert the X2. CSCsk43618
- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

  Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. CSCsi71036
- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

  Workaround: None.

  If you enter the **show policy**-**map** *name*, however, the unconditional marking actions appear. CSCsi94144
- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

  Workaround: None. CSCsl72868

- Uplinks go down when you upgrade the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

  This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

  Workarounds: To resume normal operation, do one of the following:

  – Reload both supervisor engines with the **redundancy reload shelf** command.

  – Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

  There is *no* workaround for the link flap issue. CSCsm81875

- Changing the flow control configuration with traffic and pause frames causes some traffic loss.

  This problem can happen when pause frames are sent to a switch port and the flow control receive configuration is toggled on a 10-Gigabit Ethernet port.

  Workaround: Change the flow control receive configuration when no traffic exists. CSCso71647

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

  Workaround: None. CSCsq99468

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

  You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then later allocate the same VLAN.

  Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

  Workaround: Disable native VLAN tagging on the trunk port of the switch by entering the **no switchport trunk native vlan tag** command. CSCsz12611

- Before large PACLs are fully loaded in hardware, you might observe a false completion messages like the following:

```
Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-HWPROGSUCCESS: Input Security: pacl - now
fully loaded in hardware *Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All
configured ACLs now fully loaded in hardware - hardware switching / QoS restored.
```

  Workaround: No functional impact.

  You must wait for the ACLs to be programmed before performing other TCAM related changes. CSCtd57063

- If a large number of VLAN mappings are configured, a member port might fail to join a port channel and no warming is issued.

  Workaround: Reduce the number of VLAN mappings. CSCtn56208

- WCCP service is not reacquired when a service group with a multicast group address is unconfigured, and then reconfigured.

Workaround: Configure IP multicast routing globally and establish IP PIM sparse dense mode on the CE-facing interface. CSCtl97692

- If an interface whose IP address is being used as the router ID is deleted or shuts down, and you configure a service group with a multicast group address, packet redirection to CE stops and packets are forwarded directly to the destination.

  Workaround: Unconfigure and reconfigure the service group. CSCtn88087

- Global WCCP service configuration fails to enable (WCCP global configuration is accepted but nvgen fails) on a newly deployed switch if the switch is not enabled for SVI or a Layer 3 interface.

  Workaround: Enable a Layer 3 interface in the running configuration. CSCsc88636.

- 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

- In the output of the **show interface** command, output counters for an EtherChannel member remain zero provided the ports are flapped from a peer and the switch is either Catalyst 4900M, Catalyst 4948E, or 4948E-F, or the supervisor engine is either 6E or 6L-E.

  Workaround: Enter the **show platform software interface Gix/xx statistic** command.

  CSCuf60629

Resolved Caveats in Cisco IOS Release 15.0(2)SG6

This section lists the resolved caveats in Release 15.0(2)SG6:

- 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 AC15624100000670001BC9
  ```

  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

Open Caveats for Cisco IOS Release 15.0(2)SG5

This section lists the open caveats for Cisco IOS Release 15.0(2)SG5:

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing key pair is used in the new certificate.

  On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

  Workaround: Reconnect. CSCsb11964
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

  Workaround: None. CSCsg58526
- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. CSCsg27395
- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693)
- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  Workaround: None. This is an informational message. CSCsi60898
- An IP unnumbered configuration is lost after a switch reloads.

  Workarounds: Do one of the following:
  - After a reload, copy the startup-config to the running-config.
  - Use a loopback interface as the target of the **ip unnumbered** command.

  - Change the CLI configuration so that during bootup the router port is created first.

  CSCsq63051

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

  Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. CSCsr00333

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

  Workaround: Configure an ISL/dot1q trunk port. CSCsu43445

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

  Workaround: Do one of the following:

  - Reload the standby switch again with the line card in place.
  - Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change. CSCsv44866

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  This applies to classic or E-series Catalyst 4500 supervisor engines running
  Cisco IOS Release 12.2(50)SG

  Workaround: None. CSCsw14005

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

  If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine’s MAC address table, causing possible connectivity interruption on the host.

  Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

  Workaround: None.

  The queue transmit counters as well as the policing statistics (if any) are correct. CSCsz20149

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

  This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

  Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

  The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

  CSCsz34522

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the l**auto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

  Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command. CSCta16492

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

  Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. CSCta61825

  Workaround: None CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for a Catalyst 4900M switch, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Despite the different default value, you can configure any value in the time range.

  Workaround: None. CSCte51948

- On a peer interface on a Catalyst 4948E Ethernet Switch, if errdisabled mode flap detection is set to a very small number (such as 2 flaps in 10 sec), a 10GE link flap may cause the peer interface to enter the errdisabled state.

  Workarounds: The Cisco switch default link-flap detection value is 5 flaps in 10 seconds. Use the default value or larger numbers. CSCtg07677

- After you have enabled EPM logging and the client is authenticated via MAB or Webauth, the value of AUTHTYPE is DOT1X in EPM syslog messages irrespective of the authentication method.

  Similarly, the **show epm sessions** command always displays the authentication method as DOT1X.

  Workaround: To view the authentication method used for a client, enter the **show authentication sessions** command. CSCsx42157

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

  Workaround: None. CSCso93282

- 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**, and then **no shut** on the ports. CSCtn88228

- 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

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

  Workaround: After the switch reloads, enter **shut**, and 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

- When you have two Layer 3 CE-facing interfaces, each connected to a CE to split WCCP between the CEs, and you move a WCCP service (such as 60 (ftp-native)) from one interface to the other, the target interface fails to completely transfer the service from the old to the new CE.

  Workaround: Shut down the CE-facing interface. After all of the mask-value entries point to the target CE, unshut the CE-facing interface. CSCtl09941

- 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

- 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

Not Supported on Supervisor Engine 6-E

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  Workaround: None. (CSCso68331)

Supervisor Engine 6-E and Supervisor Engine 6L-E Specific Caveats

- Occasionally, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

  Workaround: Reinsert the X2. CSCsk43618

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

  Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. CSCsi71036

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

  Workaround: None.

  If you enter the **show policy**-**map** *name*, however, the unconditional marking actions appear. CSCsi94144

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

  Workaround: None. CSCsl72868

- Uplinks go down when you upgrade the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

  This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

  Workarounds: To resume normal operation, do one of the following:

  – Reload both supervisor engines with the **redundancy reload shelf** command.

  – Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

    There is *no* workaround for the link flap issue. CSCsm81875

- Changing the flow control configuration with traffic and pause frames causes some traffic loss.

  This problem can happen when pause frames are sent to a switch port and the flow control receive configuration is toggled on a 10-Gigabit Ethernet port.

  Workaround: Change the flow control receive configuration when no traffic exists. CSCso71647

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

  Workaround: None. CSCsq99468

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

  You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then later allocate the same VLAN.

  Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

  Workaround: Disable native VLAN tagging on the trunk port of the switch by entering the **no switchport trunk native vlan tag** command. CSCsz12611

- Before large PACLs are fully loaded in hardware, you might observe a false completion messages like the following:

  ```
  Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-HWPROGSUCCESS: Input Security: pacl - now
  fully loaded in hardware *Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All
  configured ACLs now fully loaded in hardware - hardware switching / QoS restored.
  ```

  Workaround: No functional impact.

  You must wait for the ACLs to be programmed before performing other TCAM related changes. CSCtd57063

- If a large number of VLAN mappings are configured, a member port might fail to join a port channel and no warming is issued.

  Workaround: Reduce the number of VLAN mappings. CSCtn56208

- WCCP service is not reacquired when a service group with a multicast group address is unconfigured, and then reconfigured.

  Workaround: Configure IP multicast routing globally and establish IP PIM sparse dense mode on the CE-facing interface. CSCtl97692

- If an interface whose IP address is being used as the router ID is deleted or shuts down, and you configure a service group with a multicast group address, packet redirection to CE stops and packets are forwarded directly to the destination.

  Workaround: Unconfigure and reconfigure the service group. CSCtn88087

- Global WCCP service configuration fails to enable (WCCP global configuration is accepted but nvgen fails) on a newly deployed switch if the switch is not enabled for SVI or a Layer 3 interface.

  Workaround: Enable a Layer 3 interface in the running configuration. CSCsc88636.

- 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

- In the output of the **show interface** command, output counters for an EtherChannel member remain zero provided the ports are flapped from a peer and the switch is either Catalyst 4900M, Catalyst 4948E, or 4948E-F, or the supervisor engine is either 6E or 6L-E.

  Workaround: Enter the **show platform software interface Gix/xx statistic** command.

  CSCuf60629

Resolved Caveats in Cisco IOS Release 15.0(2)SG5

This section lists the resolved caveats in Release 15.0(2)SG5:

- On a switch running Cisco IOS Release 15.0(2)SG4 or 15.1(1)SG 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 15.0(2)SG4 or 15.1(1)SG 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 Release 15.0(2)SG4

This section lists the open caveats for Cisco IOS Release 15.0(2)SG4:

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing key pair is used in the new certificate.

  On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

  Workaround: Reconnect. CSCsb11964
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

  Workaround: None. CSCsg58526
- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. CSCsg27395
- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693)
- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  Workaround: None. This is an informational message. CSCsi60898
- An IP unnumbered configuration is lost after a switch reloads.

  Workarounds: Do one of the following:
  - After a reload, copy the startup-config to the running-config.
  - Use a loopback interface as the target of the **ip unnumbered** command.
  - Change the CLI configuration so that during bootup the router port is created first.

  CSCsq63051
- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. CSCsr00333

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

  Workaround: Configure an ISL/dot1q trunk port. CSCsu43445

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

  Workaround: Do one of the following:

  – Reload the standby switch again with the line card in place.

  – Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change. CSCsv44866

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

  Workaround: None. CSCsw14005

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

  If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine’s MAC address table, causing possible connectivity interruption on the host.

  Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

  Workaround: None.

  The queue transmit counters as well as the policing statistics (if any) are correct. CSCsz20149

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

  This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

  Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the l**auto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

  Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command. CSCta16492

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

  Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. CSCta61825

  Workaround: None CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for a Catalyst 4900M switch, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Despite the different default value, you can configure any value in the time range.

  Workaround: None. CSCte51948

- On a peer interface on a Catalyst 4948E Ethernet Switch, if errdisabled mode flap detection is set to a very small number (such as 2 flaps in 10 sec), a 10GE link flap may cause the peer interface to enter the errdisabled state.

  Workarounds: The Cisco switch default link-flap detection value is 5 flaps in 10 seconds. Use the default value or larger numbers. CSCtg07677

- After you have enabled EPM logging and the client is authenticated via MAB or Webauth, the value of AUTHTYPE is DOT1X in EPM syslog messages irrespective of the authentication method.

  Similarly, the **show epm sessions** command always displays the authentication method as DOT1X.

  Workaround: To view the authentication method used for a client, enter the **show authentication sessions** command. CSCsx42157

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

  Workaround: None. CSCso93282

- 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**, and then **no shut** on the ports. CSCtn88228

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

  Workaround: After the switch reloads, enter **shut**, and 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
- When you have two Layer 3 CE-facing interfaces, each connected to a CE to split WCCP between the CEs, and you move a WCCP service (such as 60 (ftp-native)) from one interface to the other, the target interface fails to completely transfer the service from the old to the new CE.

  Workaround: Shut down the CE-facing interface. After all of the mask-value entries point to the target CE, unshut the CE-facing interface. CSCtl09941
- 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
- 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
- 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

Not Supported on Supervisor Engine 6-E

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

  Workaround: None. (CSCso68331)

Supervisor Engine 6-E and Supervisor Engine 6L-E Specific Caveats

- Occasionally, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

  Workaround: Reinsert the X2. CSCsk43618
- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

  Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. CSCsi71036
- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

  Workaround: None.

  If you enter the **show policy**-**map** *name*, however, the unconditional marking actions appear. CSCsi94144
- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. CSCsl72868

- Uplinks go down when you upgrade the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

  This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

  Workarounds: To resume normal operation, do one of the following:

  – Reload both supervisor engines with the **redundancy reload shelf** command.

  – Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

  There is *no* workaround for the link flap issue. CSCsm81875

- Changing the flow control configuration with traffic and pause frames causes some traffic loss.

  This problem can happen when pause frames are sent to a switch port and the flow control receive configuration is toggled on a 10-Gigabit Ethernet port.

  Workaround: Change the flow control receive configuration when no traffic exists. CSCso71647

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

  Workaround: None. CSCsq99468

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

  You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then later allocate the same VLAN.

  Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

  Workaround: Disable native VLAN tagging on the trunk port of the switch by entering the **no switchport trunk native vlan tag** command. CSCsz12611

- Before large PACLs are fully loaded in hardware, you might observe a false completion messages like the following:

```
Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-HWPROGSUCCESS: Input Security: pacl - now
fully loaded in hardware *Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All
configured ACLs now fully loaded in hardware - hardware switching / QoS restored.
```

  Workaround: No functional impact.

  You must wait for the ACLs to be programmed before performing other TCAM related changes. CSCtd57063

- If a large number of VLAN mappings are configured, a member port might fail to join a port channel and no warming is issued.

  Workaround: Reduce the number of VLAN mappings. CSCtn56208

- WCCP service is not reacquired when a service group with a multicast group address is unconfigured, and then reconfigured.

Workaround: Configure IP multicast routing globally and establish IP PIM sparse dense mode on the CE-facing interface. CSCtl97692

- If an interface whose IP address is being used as the router ID is deleted or shuts down, and you configure a service group with a multicast group address, packet redirection to CE stops and packets are forwarded directly to the destination.

  Workaround: Unconfigure and reconfigure the service group. CSCtn88087

- Global WCCP service configuration fails to enable (WCCP global configuration is accepted but nvgen fails) on a newly deployed switch if the switch is not enabled for SVI or a Layer 3 interface.

  Workaround: Enable a Layer 3 interface in the running configuration. CSCsc88636.

- 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

- On a switch running Cisco IOS Release 15.0(2)SG4 or 15.1(1)SG 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 15.0(2)SG4 or 15.1(1)SG 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
  -

- In the output of the **show interface** command, output counters for an EtherChannel member remain zero provided the ports are flapped from a peer and the switch is either Catalyst 4900M, Catalyst 4948E, or 4948E-F, or the supervisor engine is either 6E or 6L-E.

  Workaround: Enter the **show platform software interface Gix/xx statistic** command.

  CSCuf60629

Resolved Caveats in Cisco IOS Release 15.0(2)SG4

This section lists the resolved caveats in Release 15.0(2)SG4:

- If two clients are authenticated by MAB on a multi-host port, when the first client moves to a different port using MAC Move, the second host is not authenticated; it remains in the running state.

  Workaround: Clear the MAC address. CSCtn24046

- 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

Open Caveats for Cisco IOS Release 15.0(2)SG3

This section lists the open caveats for Cisco IOS Release 15.0(2)SG3:

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing key pair is used in the new certificate.

  On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

  Workaround: Reconnect. CSCsb11964

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

  Workaround: None. CSCsg58526

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

Workaround: Enter the **no shutdown** command. CSCsg27395

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  Workaround: None. This is an informational message. CSCsi60898

- An IP unnumbered configuration is lost after a switch reloads.

  Workarounds: Do one of the following:

  – After a reload, copy the startup-config to the running-config.

  – Use a loopback interface as the target of the **ip unnumbered** command.

  – Change the CLI configuration so that during bootup the router port is created first.

  CSCsq63051

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. CSCsr00333

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

  Workaround: Configure an ISL/dot1q trunk port. CSCsu43445

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

  Workaround: Do one of the following:

  – Reload the standby switch again with the line card in place.

  – Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change. CSCsv44866

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

  ```
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  ```

  This applies to classic or E-series Catalyst 4500 supervisor engines running
  Cisco IOS Release 12.2(50)SG

Workaround: None. CSCsw14005

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

  If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine’s MAC address table, causing possible connectivity interruption on the host.

  Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

  Workaround: None.

  The queue transmit counters as well as the policing statistics (if any) are correct. CSCsz20149

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

  This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

  Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

  The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

  CSCsz34522

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **lauto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

  Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command. CSCta16492

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

  Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. CSCta61825

  Workaround: None CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for a Catalyst 4900M switch, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Despite the different default value, you can configure any value in the time range.

Workaround: None. CSCte51948

- On a peer interface on a Catalyst 4948E Ethernet Switch, if errdisabled mode flap detection is set to a very small number (such as 2 flaps in 10 sec), a 10GE link flap may cause the peer interface to enter the errdisabled state.

  Workarounds: The Cisco switch default link-flap detection value is 5 flaps in 10 seconds. Use the default value or larger numbers. CSCtg07677
- After you have enabled EPM logging and the client is authenticated via MAB or Webauth, the value of AUTHTYPE is DOT1X in EPM syslog messages irrespective of the authentication method.

  Similarly, the **show epm sessions** command always displays the authentication method as DOT1X.

  Workaround: To view the authentication method used for a client, enter the **show authentication sessions** command. CSCsx42157
- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

  Workaround: None. CSCso93282
- 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**, and then **no shut** on the ports. CSCtn88228
- 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
- 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 reboot a switch, the configured value of the interface MTU size on the members of the port channel interface does not function for IPv6 traffic.

  Workaround: After the switch reloads, enter **shut**, and 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

- When you have two Layer 3 CE-facing interfaces, each connected to a CE to split WCCP between the CEs, and you move a WCCP service (such as 60 (ftp-native)) from one interface to the other, the target interface fails to completely transfer the service from the old to the new CE.

  Workaround: Shut down the CE-facing interface. After all of the mask-value entries point to the target CE, unshut the CE-facing interface. CSCtl09941

- 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

- 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

- 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

Not Supported on Supervisor Engine 6-E

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  Workaround: None. (CSCso68331)

Supervisor Engine 6-E and Supervisor Engine 6L-E Specific Caveats

- Occasionally, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

  Workaround: Reinsert the X2. CSCsk43618

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. CSCsi71036

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

  Workaround: None.

  If you enter the **show policy**-**map** *name*, however, the unconditional marking actions appear. CSCsi94144

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

  Workaround: None. CSCsl72868

- Uplinks go down when you upgrade the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

  This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

  Workarounds: To resume normal operation, do one of the following:

  – Reload both supervisor engines with the **redundancy reload shelf** command.

  – Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

  There is *no* workaround for the link flap issue. CSCsm81875

- Changing the flow control configuration with traffic and pause frames causes some traffic loss.

  This problem can happen when pause frames are sent to a switch port and the flow control receive configuration is toggled on a 10-Gigabit Ethernet port.

  Workaround: Change the flow control receive configuration when no traffic exists. CSCso71647

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

  Workaround: None. CSCsq99468

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

  You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then later allocate the same VLAN.

  Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

  Workaround: Disable native VLAN tagging on the trunk port of the switch by entering the **no switchport trunk native vlan tag** command. CSCsz12611

- Before large PACLs are fully loaded in hardware, you might observe a false completion messages like the following:

```
Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-HWPROGSUCCESS: Input Security: pacl - now
fully loaded in hardware *Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All
configured ACLs now fully loaded in hardware - hardware switching / QoS restored.
```

Workaround: No functional impact.

You must wait for the ACLs to be programmed before performing other TCAM related changes. CSCtd57063

- If a large number of VLAN mappings are configured, a member port might fail to join a port channel and no warming is issued.

  Workaround: Reduce the number of VLAN mappings. CSCtn56208
- WCCP service is not reacquired when a service group with a multicast group address is unconfigured, and then reconfigured.

  Workaround: Configure IP multicast routing globally and establish IP PIM sparse dense mode on the CE-facing interface. CSCtl97692
- If an interface whose IP address is being used as the router ID is deleted or shuts down, and you configure a service group with a multicast group address, packet redirection to CE stops and packets are forwarded directly to the destination.

  Workaround: Unconfigure and reconfigure the service group. CSCtn88087
- Global WCCP service configuration fails to enable (WCCP global configuration is accepted but nvgen fails) on a newly deployed switch if the switch is not enabled for SVI or a Layer 3 interface.

  Workaround: Enable a Layer 3 interface in the running configuration. CSCsc88636.
- 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
- If two clients are authenticated by MAB on a multi-host port, when the first client moves to a different port using MAC Move, the second host is not authenticated; it remains in the running state.

  Workaround: Clear the MAC address. CSCtn24046
- In the output of the **show interface** command, output counters for an EtherChannel member remain zero provided the ports are flapped from a peer and the switch is either Catalyst 4900M, Catalyst 4948E, or 4948E-F, or the supervisor engine is either 6E or 6L-E.

  Workaround: Enter the **show platform software interface Gix/xx statistic** command.

  CSCuf60629

Resolved Caveats in Cisco IOS Release 15.0(2)SG3

This section lists the resolved caveats in Release 15.0(2)SG3:

- When only an RX fiber is broken on a 10-Gigabit Ethernet link in a REP ring, REP segment convergence might require more than 500 ms.

  Only WS-C4900M uplink ports (Te1/1-8), WS-X45-SUP6L-E uplink ports, and WS-X4904-10GE are affected.

  Workaround: Use a non-affected module for REP ports such as WS-X4908-10GE. CSCtr76579

- 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

- A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS Software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:

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

  CSCtr91106

Open Caveats for Cisco IOS Release 15.0(2)SG2

This section lists the open caveats for Cisco IOS Release 15.0(2)SG2:

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing key pair is used in the new certificate.

  On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. CSCsb11964

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

  Workaround: None. CSCsg58526

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. CSCsg27395

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

  Workaround: None. This is an informational message. CSCsi60898

- An IP unnumbered configuration is lost after a switch reloads.

  Workarounds: Do one of the following:

  - After a reload, copy the startup-config to the running-config.
  - Use a loopback interface as the target of the **ip unnumbered** command.
  - Change the CLI configuration so that during bootup the router port is created first.

  CSCsq63051

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

  Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. CSCsr00333

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

  Workaround: Configure an ISL/dot1q trunk port. CSCsu43445

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

  Workaround: Do one of the following:

  - Reload the standby switch again with the line card in place.
  - Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change. CSCsv44866

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

  ```
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  ```

  This applies to classic or E-series Catalyst 4500 supervisor engines running
  Cisco IOS Release 12.2(50)SG

  Workaround: None. CSCsw14005

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

  If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

  Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

  Workaround: None.

  The queue transmit counters as well as the policing statistics (if any) are correct. CSCsz20149

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

  This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

  Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

  The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

  CSCsz34522

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the
  lauto qos voice trust command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

  Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command. CSCta16492

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. CSCta61825

Workaround: None CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for a Catalyst 4900M switch, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Despite the different default value, you can configure any value in the time range.

  Workaround: None. CSCte51948

- On a peer interface on a Catalyst 4948E Ethernet Switch, if errdisabled mode flap detection is set to a very small number (such as 2 flaps in 10 sec), a 10GE link flap may cause the peer interface to enter the errdisabled state.

  Workarounds: The Cisco switch default link-flap detection value is 5 flaps in 10 seconds. Use the default value or larger numbers. CSCtg07677

- After you have enabled EPM logging and the client is authenticated via MAB or Webauth, the value of AUTHTYPE is DOT1X in EPM syslog messages irrespective of the authentication method.

  Similarly, the **show epm sessions** command always displays the authentication method as DOT1X.

  Workaround: To view the authentication method used for a client, enter the **show authentication sessions** command. CSCsx42157

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

  Workaround: None. CSCso93282

- 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**, and then **no shut** on the ports. CSCtn88228

- 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

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

  Workaround: After the switch reloads, enter **shut**, and 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

- When you have two Layer 3 CE-facing interfaces, each connected to a CE to split WCCP between the CEs, and you move a WCCP service (such as 60 (ftp-native)) from one interface to the other, the target interface fails to completely transfer the service from the old to the new CE.

  Workaround: Shut down the CE-facing interface. After all of the mask-value entries point to the target CE, unshut the CE-facing interface. CSCtl09941

- 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

- 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

- 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

Not Supported on Supervisor Engine 6-E

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  Workaround: None. (CSCso68331)

Supervisor Engine 6-E and Supervisor Engine 6L-E Specific Caveats

- Occasionally, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

  Workaround: Reinsert the X2. CSCsk43618

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

  Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. CSCsi71036

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

  Workaround: None.

  If you enter the **show policy**-**map** *name*, however, the unconditional marking actions appear. CSCsi94144

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

  Workaround: None. CSCsl72868

- Uplinks go down when you upgrade the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

  This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

  Workarounds: To resume normal operation, do one of the following:

  – Reload both supervisor engines with the **redundancy reload shelf** command.

  – Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

    There is *no* workaround for the link flap issue. CSCsm81875

- Changing the flow control configuration with traffic and pause frames causes some traffic loss.

  This problem can happen when pause frames are sent to a switch port and the flow control receive configuration is toggled on a 10-Gigabit Ethernet port.

  Workaround: Change the flow control receive configuration when no traffic exists. CSCso71647

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

  Workaround: None. CSCsq99468

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

  You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then later allocate the same VLAN.

  Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

  Workaround: Disable native VLAN tagging on the trunk port of the switch by entering the **no switchport trunk native vlan tag** command. CSCsz12611

- Before large PACLs are fully loaded in hardware, you might observe a false completion messages like the following:

  ```
  Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-HWPROGSUCCESS: Input Security: pacl - now
  fully loaded in hardware *Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All
  configured ACLs now fully loaded in hardware - hardware switching / QoS restored.
  ```

  Workaround: No functional impact.

  You must wait for the ACLs to be programmed before performing other TCAM related changes. CSCtd57063

- If a large number of VLAN mappings are configured, a member port might fail to join a port channel and no warming is issued.

  Workaround: Reduce the number of VLAN mappings. CSCtn56208

- WCCP service is not reacquired when a service group with a multicast group address is unconfigured, and then reconfigured.

  Workaround: Configure IP multicast routing globally and establish IP PIM sparse dense mode on the CE-facing interface. CSCtl97692

- If an interface whose IP address is being used as the router ID is deleted or shuts down, and you configure a service group with a multicast group address, packet redirection to CE stops and packets are forwarded directly to the destination.

  Workaround: Unconfigure and reconfigure the service group. CSCtn88087

- Global WCCP service configuration fails to enable (WCCP global configuration is accepted but nvgen fails) on a newly deployed switch if the switch is not enabled for SVI or a Layer 3 interface.

  Workaround: Enable a Layer 3 interface in the running configuration. CSCsc88636.

- 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

- When only an RX fiber is broken on a 10-Gigabit Ethernet link in a REP ring, REP segment convergence might require more than 500 ms.

  Only WS-C4900M uplink ports (Te1/1-8), WS-X45-SUP6L-E uplink ports, and WS-X4904-10GE are affected.

  Workaround: Use a non-affected module for REP ports such as WS-X4908-10GE. CSCtr76579

- If two clients are authenticated by MAB on a multi-host port, when the first client moves to a different port using MAC Move, the second host is not authenticated; it remains in the running state.

  Workaround: Clear the MAC address. CSCtn24046

- In the output of the **show interface** command, output counters for an EtherChannel member remain zero provided the ports are flapped from a peer and the switch is either Catalyst 4900M, Catalyst 4948E, or 4948E-F, or the supervisor engine is either 6E or 6L-E.

Workaround: Enter the **show platform software interface Gix/xx statistic** command.

CSCuf60629

Resolved Caveats in Cisco IOS Release 15.0(2)SG2

This section lists the resolved caveats in Release 15.0(2)SG2:

- 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 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
- 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
- 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
- Typically, when a switch crashes, the crashinfo file is empty. Occasionally, the following text is present:

  ```
  Last reload status: 00000C00 020D0000
  ```

  Workaround: Attach the console to collect additional crash data. CSCtu05426
- When you enter the **rep preempt segment** command, the MAC might not flush.

  Workaround: Re-enter the **rep preempt segment** command. CSCtr89862
- 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

- A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS Software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:

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

  CSCtr91106

Open Caveats for Cisco IOS Release 15.0(2)SG1

This section lists the open caveats for Cisco IOS Release 15.0(2)SG1:

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing key pair is used in the new certificate.

  On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

  Workaround: Reconnect. CSCsb11964

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

  Workaround: None. CSCsg58526

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. CSCsg27395
- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693)
- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  Workaround: None. This is an informational message. CSCsi60898
- An IP unnumbered configuration is lost after a switch reloads.

  Workarounds: Do one of the following:

  – After a reload, copy the startup-config to the running-config.

  – Use a loopback interface as the target of the **ip unnumbered** command.

  – Change the CLI configuration so that during bootup the router port is created first.

  CSCsq63051
- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. CSCsr00333
- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

  Workaround: Configure an ISL/dot1q trunk port. CSCsu43445
- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

  Workaround: Do one of the following:

  – Reload the standby switch again with the line card in place.

  – Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change. CSCsv44866
- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

  ```
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  ```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. CSCsw14005

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

  If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

  Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

  Workaround: None.

  The queue transmit counters as well as the policing statistics (if any) are correct. CSCsz20149

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

  This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

  Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

  The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

  CSCsz34522

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the l**auto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

  Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command. CSCta16492

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

  Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. CSCta61825

  Workaround: None CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for a Catalyst 4900M switch, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Despite the different default value, you can configure any value in the time range.

Workaround: None. CSCte51948

- On a peer interface on a Catalyst 4948E Ethernet Switch, if errdisabled mode flap detection is set to a very small number (such as 2 flaps in 10 sec), a 10GE link flap may cause the peer interface to enter the errdisabled state.

  Workarounds: The Cisco switch default link-flap detection value is 5 flaps in 10 seconds. Use the default value or larger numbers. CSCtg07677

- After you have enabled EPM logging and the client is authenticated via MAB or Webauth, the value of AUTHTYPE is DOT1X in EPM syslog messages irrespective of the authentication method.

  Similarly, the **show epm sessions** command always displays the authentication method as DOT1X.

  Workaround: To view the authentication method used for a client, enter the **show authentication sessions** command. CSCsx42157

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

  Workaround: None. CSCso93282

- 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**, and then **no shut** on the ports. CSCtn88228

- 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

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

  Workaround: After the switch reloads, enter **shut**, and 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

- When you have two Layer 3 CE-facing interfaces, each connected to a CE to split WCCP between the CEs, and you move a WCCP service (such as 60 (ftp-native)) from one interface to the other, the target interface fails to completely transfer the service from the old to the new CE.

  Workaround: Shut down the CE-facing interface. After all of the mask-value entries point to the target CE, unshut the CE-facing interface. CSCtl09941
- 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
- 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
- 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
- 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
- When you enter the **rep preempt segment** command, the MAC might not flush.

  Workaround: Re-enter the **rep preempt segment** command. CSCtr89862
- 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

- 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

Not Supported on Supervisor Engine 6-E

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  Workaround: None. CSCso68331
- 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
- Typically, when a switch crashes, the crashinfo file is empty. Occasionally, the following text is present:

  ```
  Last reload status: 00000C00 020D0000
  ```

  Workaround: Attach the console to collect additional crash data. CSCtu05426

Supervisor Engine 6-E and Supervisor Engine 6L-E Specific Caveats

- Occasionally, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

  Workaround: Reinsert the X2. CSCsk43618
- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

  Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. CSCsi71036
- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

  Workaround: None.

  If you enter the **show policy**-**map** *name*, however, the unconditional marking actions appear. CSCsi94144
- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

  Workaround: None. CSCsl72868
- Uplinks go down when you upgrade the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

  – Reload both supervisor engines with the **redundancy reload shelf** command.
  – Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

  There is *no* workaround for the link flap issue. CSCsm81875

- Changing the flow control configuration with traffic and pause frames causes some traffic loss.

  This problem can happen when pause frames are sent to a switch port and the flow control receive configuration is toggled on a 10-Gigabit Ethernet port.

  Workaround: Change the flow control receive configuration when no traffic exists. CSCso71647

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

  Workaround: None. CSCsq99468

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

  You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then later allocate the same VLAN.

  Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

  Workaround: Disable native VLAN tagging on the trunk port of the switch by entering the **no switchport trunk native vlan tag** command. CSCsz12611

- Before large PACLs are fully loaded in hardware, you might observe a false completion messages like the following:

```
Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-HWPROGSUCCESS: Input Security: pacl - now
fully loaded in hardware *Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All
configured ACLs now fully loaded in hardware - hardware switching / QoS restored.
```

  Workaround: No functional impact.

  You must wait for the ACLs to be programmed before performing other TCAM related changes. CSCtd57063

- If a large number of VLAN mappings are configured, a member port might fail to join a port channel and no warming is issued.

  Workaround: Reduce the number of VLAN mappings. CSCtn56208

- WCCP service is not reacquired when a service group with a multicast group address is unconfigured, and then reconfigured.

  Workaround: Configure IP multicast routing globally and establish IP PIM sparse dense mode on the CE-facing interface. CSCtl97692

- If an interface whose IP address is being used as the router ID is deleted or shuts down, and you configure a service group with a multicast group address, packet redirection to CE stops and packets are forwarded directly to the destination.

  Workaround: Unconfigure and reconfigure the service group. CSCtn88087
- Global WCCP service configuration fails to enable (WCCP global configuration is accepted but nvgen fails) on a newly deployed switch if the switch is not enabled for SVI or a Layer 3 interface.

  Workaround: Enable a Layer 3 interface in the running configuration. CSCsc88636.
- 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
- When only an RX fiber is broken on a 10-Gigabit Ethernet link in a REP ring, REP segment convergence might require more than 500 ms.

  Only WS-C4900M uplink ports (Te1/1-8), WS-X45-SUP6L-E uplink ports, and WS-X4904-10GE are affected.

  Workaround: Use a non-affected module for REP ports such as WS-X4908-10GE. CSCtr76579
- If two clients are authenticated by MAB on a multi-host port, when the first client moves to a different port using MAC Move, the second host is not authenticated; it remains in the running state.

  Workaround: Clear the MAC address. CSCtn24046
- In the output of the **show interface** command, output counters for an EtherChannel member remain zero provided the ports are flapped from a peer and the switch is either Catalyst 4900M, Catalyst 4948E, or 4948E-F, or the supervisor engine is either 6E or 6L-E.

  Workaround: Enter the **show platform software interface Gix/xx statistic** command.

  CSCuf60629

Resolved Caveats in Cisco IOS Release 15.0(2)SG1

This section lists the resolved caveats in Release 15.0(2)SG1:

- If you use MDA or multi-auth host mode with authentication open, the switch ignores unicast EAPOL responses.

  Workarounds:
  - Force the supplicant to use multicast EAPOL.
  - Do not use authentication open mode.

  CSCtq33048
- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

  Workaround: None. CSCsy72343
- When Fallback WebAuth and Multi-host are configured on a port and no PACL exists, **permit ip any any** is installed in the TCAM and all traffic from the host is allowed to pass.

  Workaround: Configure an ACL on the port. CSCte18760

- 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

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

  Workaround: Do not configure open directive on the switch.

  CSCto48824

- When reconnecting 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 duplicate address register issue is usually triggered by disconnecting or reconnecting.

  Workaround: Disable gratuitous ARP on the Windows device. CSCtn27420

- If you create a new IPv6 ACL, delete a permit ACE, and then re-add 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 this output, **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

- Selective Q-in-Q CLIs are rejected on a port channel after deleting all the one-to-one CLIs.

  Workaround: Enter the **interface range** command to configure all member ports to use a new port channel that is created automatically. CSCtn52362

- A port channel does not come up after you configure for VLAN translation.

  Workaround: Enter **shut**, and then **no shut** on the member port. CSCtn52404

- ND/NS packets are dropped when an IPv6 ACL is attached to an Layer 3 interface.

  Workaround: Add the following permit ACEs to the ACL:

  ```
     permit icmp any any nd-ns
      permit icmp any any nd-na
  ```

  CSCtg77035

- 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

- Memory leak is observed in the RADIUS and EAP framework processes. The output of the **show mem all totals** command displays the name of the leaked memory as AAA Attr String and AAA Attr List.

  Workaround: None CSCto34321

- When QoS commands are applied line by line on PVLAN isolated trunks, the policer is not applied and line rate traffic exits the port.

  Workaround: Cut and paste the configuration. Then apply rapidly to PVLAN isolated trunk port. CSCtq04058

- When you make QoS-related changes, a Catalyst 4500 switch may reload unexpectedly.

  Workaround: None. CSCtn77500

- When the active port set to the egress policy is single, you cannot modify the multicast control packets (like HSRP/OSPF) IP ToS field.

  Workaround: None. CSCtg60011

- When a connected data device behind a phone disconnects from a port configured for multi-auth host mode, a new session for the device is restarted even though the device is absent.

  The CDP TLV generated to indicate that a data device has disconnected is ignored. This is done to avoid disconnecting other connected data clients, if any. (Refer to CSCta47293.)

  Workarounds: Enter either of the following commands:

  – **clear authentication session interface**

  – **authentication timer inactivity**

  CSCtg83631

- 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

- RA Guard counters are not incremented in the output of the **show ipv6 first-hop counters interface** command when Router Advertisement and Router Redirect packets with Destination address FF02::x are dropped.

  Workaround: None. CSCtf69108

Open Caveats for Cisco IOS Release 15.0(2)SG

This section lists the open caveats for Cisco IOS Release 15.0(2)SG:

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing key pair is used in the new certificate.

  On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

  Workaround: Reconnect. CSCsb11964
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

  Workaround: None. CSCsg58526
- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. CSCsg27395
- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. CSCse34693
- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  Workaround: None. This is an informational message. (CSCsi60898)
- An IP unnumbered configuration is lost after a switch reloads.

  Workarounds: Do one of the following:
  - After a reload, copy the startup-config to the running-config.
  - Use a loopback interface as the target of the **ip unnumbered** command.
  - Change the CLI configuration so that during bootup the router port is created first.

  CSCsq63051
- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. CSCsr00333

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

  Workaround: Configure an ISL/dot1q trunk port. CSCsu43445

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

  Workaround: Do one of the following:

  – Reload the standby switch again with the line card in place.

  – Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change. CSCsv44866

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

  Workaround: None. CSCsw14005

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

  If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

  Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

  Workaround: None. CSCsy72343

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

  Workaround: None.

  The queue transmit counters as well as the policing statistics (if any) are correct. CSCsz20149

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the l**auto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

  Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command. CSCta16492

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

  Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. CSCta61825

  Workaround: None CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for a Catalyst 4900M switch, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Despite the different default value, you can configure any value in the time range.

  Workaround: None. CSCte51948

- On a peer interface on a Catalyst 4948E Ethernet Switch, if errdisabled mode flap detection is set to a very small number (such as 2 flaps in 10 sec), a 10GE link flap may cause the peer interface to enter the errdisabled state.

  Workarounds: The Cisco switch default link-flap detection value is 5 flaps in 10 seconds. Use the default value or larger numbers. CSCtg07677

- When a connected data device behind a phone disconnects from a port configured for multi-auth host mode, a new session for the device is restarted even though the device is absent.

  The CDP TLV generated to indicate that a data device has disconnected is ignored. This is done to avoid disconnecting other connected data clients, if any. (Refer to CSCta47293.)

  Workarounds: Enter either of the following commands:

  – **clear authentication session interface**

  – **authentication timer inactivity**

  CSCtg83631

- When Fallback WebAuth and Multi-host are configured on a port and no PACL exists, **permit ip any any** is installed in the TCAM and all traffic from the host is allowed to pass.

  Workaround: Configure an ACL on the port. CSCte18760

- After you have enabled EPM logging and the client is authenticated via MAB or Webauth, the value of AUTHTYPE is DOT1X in EPM syslog messages irrespective of the authentication method.

Similarly, the **show epm sessions** command always displays the authentication method as DOT1X.

Workaround: To view the authentication method used for a client, enter the **show authentication sessions** command. CSCsx42157

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

  Workaround: None. CSCso93282

- 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**, and then **no shut** on the ports. CSCtn88228

- 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

- 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

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

  Workaround: Do not configure open directive on the switch.

  CSCto48824

- When reconnecting 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 duplicate address register issue is usually triggered by disconnecting or reconnecting.

  Workaround: Disable gratuitous ARP on the Windows device. CSCtn27420

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

  Workaround: After the switch reloads, enter **shut**, and 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

- If you create a new IPv6 ACL, delete a permit ACE, and then re-add 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 this output, **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

- When you have two Layer 3 CE-facing interfaces, each connected to a CE to split WCCP between the CEs, and you move a WCCP service (such as 60 (ftp-native)) from one interface to the other, the target interface fails to completely transfer the service from the old to the new CE.

  Workaround: Shut down the CE-facing interface. After all of the mask-value entries point to the target CE, unshut the CE-facing interface. CSCtl09941

- Selective Q-in-Q CLIs are rejected on a port channel after deleting all the one-to-one CLIs.

  Workaround: Enter the **interface range** command to configure all member ports to use a new port channel that is created automatically. CSCtn52362

- A port channel does not come up after you configure for VLAN translation.

  Workaround: Enter **shut**, and then **no shut** on the member port. CSCtn52404

- 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

- 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 you enter the **rep preempt segment** command, the MAC might not flush.

  Workaround: Re-enter the **rep preempt segment** command. CSCtr89862
- 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
- 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

- 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

Not Supported on Supervisor Engine 6-E

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  Workaround: None. CSCso68331

- Typically, when a switch crashes, the crashinfo file is empty. Occasionally, the following text is present:

  ```
  Last reload status: 00000C00 020D0000
  ```

  Workaround: Attach the console to collect additional crash data. CSCtu05426

Supervisor Engine 6-E and Supervisor Engine 6L-E Specific Caveats

- Occasionally, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

  Workaround: Reinsert the X2. (CSCsk43618)
- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

  Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. CSCsi71036
- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

  Workaround: None.

  If you enter the **show policy**-**map** *name*, however, the unconditional marking actions appear. CSCsi94144
- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

  Workaround: None. CSCsl72868
- Uplinks go down when you upgrade the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

  This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

  Workarounds: To resume normal operation, do one of the following:

  – Reload both supervisor engines with the **redundancy reload shelf** command.

  – Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

  There is *no* workaround for the link flap issue. CSCsm81875
- Changing the flow control configuration with traffic and pause frames causes some traffic loss.

  This problem can happen when pause frames are sent to a switch port and the flow control receive configuration is toggled on a 10-Gigabit Ethernet port.

  Workaround: Change the flow control receive configuration when no traffic exists. CSCso71647
- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

  Workaround: None. CSCsq99468
- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then later allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

  Workaround: Disable native VLAN tagging on the trunk port of the switch by entering the **no switchport trunk native vlan tag** command. CSCsz12611

- Before large PACLs are fully loaded in hardware, you might observe a false completion messages like the following:

  ```
  Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-HWPROGSUCCESS: Input Security: pacl - now
  fully loaded in hardware *Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All
  configured ACLs now fully loaded in hardware - hardware switching / QoS restored.
  ```

  Workaround: No functional impact.

  You must wait for the ACLs to be programmed before performing other TCAM related changes. CSCtd57063

- RA Guard counters are not incremented in the output of the **show ipv6 first-hop counters interface** command when Router Advertisement and Router Redirect packets with Destination address FF02::x are dropped.

  Workaround: None. CSCtf69108

- ND/NS packets are dropped when an IPv6 ACL is attached to an Layer 3 interface.

  Workaround: Add the following permit ACEs to the ACL:

  ```
     permit icmp any any nd-ns
      permit icmp any any nd-na
  ```

  CSCtg77035

- If a port has joined a port channel, you cannot modify a VLAN map configuration of an EtherChannel member port.

  Workaround: Shut the member port. CSCtn49832

- If a large number of VLAN mappings are configured, a member port might fail to join a port channel and no warming is issued.

  Workaround: Reduce the number of VLAN mappings. CSCtn56208

- WCCP service is not reacquired when a service group with a multicast group address is unconfigured, and then reconfigured.

  Workaround: Configure IP multicast routing globally and establish IP PIM sparse dense mode on the CE-facing interface. CSCtl97692

- If an interface whose IP address is being used as the router ID is deleted or shuts down, and you configure a service group with a multicast group address, packet redirection to CE stops and packets are forwarded directly to the destination.

  Workaround: Unconfigure and reconfigure the service group. CSCtn88087

- Global WCCP service configuration fails to enable (WCCP global configuration is accepted but nvgen fails) on a newly deployed switch if the switch is not enabled for SVI or a Layer 3 interface.

  Workaround: Enable a Layer 3 interface in the running configuration. CSCsc88636.

- 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
- When only an RX fiber is broken on a 10-Gigabit Ethernet link in a REP ring, REP segment convergence might require more than 500 ms.

  Only WS-C4900M uplink ports (Te1/1-8), WS-X45-SUP6L-E uplink ports, and WS-X4904-10GE are affected.

  Workaround: Use a non-affected module for REP ports such as WS-X4908-10GE. CSCtr76579
- If two clients are authenticated by MAB on a multi-host port, when the first client moves to a different port using MAC Move, the second host is not authenticated; it remains in the running state.

  Workaround: Clear the MAC address. CSCtn24046
- In the output of the **show interface** command, output counters for an EtherChannel member remain zero provided the ports are flapped from a peer and the switch is either Catalyst 4900M, Catalyst 4948E, or 4948E-F, or the supervisor engine is either 6E or 6L-E.

  Workaround: Enter the **show platform software interface Gix/xx statistic** command.

  CSCuf60629

Resolved Caveats in Cisco IOS Release 15.0(2)SG

This section lists the resolved caveats in Release 15.0(2)SG:

- If you reconfigure VLAN load balancing to reflect different blocking ports, when VLAN load balancing is progressing, manual preemption does not occur.

  Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

  a. Reconfigure the VLAN load balancing configuration on the desired REP ports.

  b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.

  c. Use the **no shut** command on the same port to restore normal REP topology with one ALT port.

  d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

  CSCsv69853
- When you remove an SFP+ from a OneX converter in a X2 slot, the system requires approximately 45 seconds to recognize this action. During this interval, all commands reflect that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause the “duplicate seeprom” error message to appear.

  Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:
  - Enter any commands for that port.
  - Insert an SFP+ in that port.
  - Reinsert the removed SFP+ in another port. CSCsv90044

- If you disable and reenable IGMP snooping on a VLAN, the output of the **show mac address** command does not associate the term “Switch” with the multicast entry. Multicast traffic is not impacted.

  Workaround: Enter **shut**, and then **no shut** on the SVI. CSCtg72559

- If an X2 or SFP is in an inactive uplink port on a Supervisor Engine V-10GE, Supervisor II+10GE, Supervisor 6-E, or Supervisor 6-LE, it might cause threshold violations to be reported once every 10 minutes.

  Workaround: Remove the X2 or SFP from the port. CSCth08212

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

  Workaround: None. CSCtj56811

- A switch might fail while loading BGP routes if the **ip cef accounting non-recursive** command is already configured.

  Workaround: Disable the **ip cef accounting non-recursive** command. CSCtn68186

- When CX1 or SFP+ is plugged into a OneX converter (CVR-X2-SFP10G) in a WS-X4908-10GE, the switch requires 1 minute to boot the link.

  Workaround: None. CSCtc46340

- A switch fails when attaching a service policy to a target, if the service policy contains more than 56 classes and each class is associated with an explicit marking action. For example:

  ```
  policy-map pm
   class c0
     set dscp default
     set cos 0
   class c1
     set dscp 1
     set cos 1
   class c2
     set dscp 2
     set cos 2
  ... ...
   class c56
     set dscp cs7
     set cos 0
  ```

  Workaround: Use tablemap-based marking. CSC99836

- When you reload an adjoining Catalyst 3400 switch connected to two Catalyst 4500 Series switches in a REP ring topology, the REP alternate port does not block any traffic.

  Workaround: Enter **shut**, and then **no shut** on the alternate port. CSCtn26322

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

  Workaround: None. CSCtn61307

- A nonsupplicant 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 the client reattempts 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 configuration, the VLANs that are not already in the VLAN database are not created.

Workarounds:

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

- After reloading and rebooting one of the switches in a REP ring topology, the alternate port forwards traffic and causes a loop.

  Workaround: Enter **shut**, and then **no shut** on the alternate interface. CSCtn03533

- If VLAN load balancing is enabled, after the primary Flex Link goes down and then recovers, a Catalyst 4500 switch sends out multicast frames when the preemption timer expires. The switch sends out one additional unicast frame after it sends out the Flex Link multicast frames, causing the secondary core to learn the MAC address on an incorrect port.

  Workaround: None. CSCtk30811

- LACP ports between a Catalyst 4500 switch and a Nexus switch 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

Troubleshooting

These sections provide troubleshooting guidelines for the Catalyst 4000 family running IOS supervisor engines:

- Netbooting from the ROMMON, page 125
- Troubleshooting at the System Level, page 126
- Troubleshooting Modules, page 126
- Troubleshooting MIBs, page 127

Netbooting from the ROMMON

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

1. Boot from a CompactFlash 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 image name cat4000-is-mz.160 located on the TFTP server 172.16.1.8, enter the following command:

```
rommon 3> boot tftp://172.16.1.8/tftpboot/cat4000-is-mz
```

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 in all Catalyst 4500 Cisco IOS releases. 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.

Related Documentation

Although their Release Notes are unique, the 4 platforms (Catalyst 4500, Catalyst 4900, Catalyst ME 4900, and Catalyst 4900M) use the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide*. Refer to the following home pages for additional information:

- Catalyst 4500 Series Switch Documentation Home

  http://www.cisco.com/go/cat4500/docs
- Catalyst 4900 Series Switch Documentation Home

  http://www.cisco.com/go/cat4900/docs
- Cisco ME 4900 Series Ethernet Switches Documentation Home

  http://www.cisco.com/en/US/products/ps7009/tsd_products_support_series_home.html

Hardware Documents

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

- *Catalyst 4500 Series Switches Installation Guide*

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/installation/guide/78-14409-08/4500inst.html
- *Catalyst 4500 E-series Switches Installation Guide*

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/catalyst4500e/installation/guide/Eseries.html
- For information about individual switching modules and supervisors, refer to the *Catalyst 4500 Series Module Installation Guide* at:

  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html
- *Regulatory Compliance and Safety Information for the Catalyst 4500 Series Switches*

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/regulatory/compliance/78_13233.html
- Installation notes for specific supervisor engines or for accessory hardware are available at:

http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html

- Catalyst 4900 and 4900M hardware installation information is available at:

  http://www.cisco.com/en/US/products/ps6021/prod_installation_guides_list.html

- Cisco ME 4900 Series Ethernet Switches installation information is available at:

  http://www.cisco.com/en/US/products/ps7009/prod_installation_guides_list.html

Software Documentation

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

- Catalyst 4500 release notes are available at:

  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_release_notes_list.html

- Catalyst 4900 release notes are available at:

  http://www.cisco.com/en/US/products/ps6021/prod_release_notes_list.html

- Cisco ME4900 4900 Series Ethernet Switch release notes are available at:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_11511.html

Software documents for the Catalyst 4500 Classic, Catalyst 4500 E-Series, Catalyst 4900, and Cisco ME 4900 Series Ethernet Switches are available at the following URLs:

- *Catalyst 4500 Series Software Configuration Guide*

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

- *Catalyst 4500 Series Software Command Reference*

  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_command_reference_list.html

- *Catalyst 4500 Series Software System Message Guide*

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_system_message_guides_list.html

Cisco IOS Documentation

Platform-independent Cisco IOS documentation may also apply to the Catalyst 4500 and 4900 switches. These documents are available at the following URLs:

- Cisco IOS configuration guides, Release 12.x

  http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html

- Cisco IOS command references, Release 12.x

  http://www.cisco.com/en/US/products/ps6350/prod_command_reference_list.html

  You can also use the Command Lookup Tool at:

  http://tools.cisco.com/Support/CLILookup/cltSearchAction.do

- Cisco IOS system messages, version 12.x

  http://www.cisco.com/en/US/products/ps6350/products_system_message_guides_list.html

You can also use the Error Message Decoder tool at:

http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

- For information about MIBs, refer to:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

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:

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

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

Original SSLeay License:

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

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

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

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

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

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

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

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

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

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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

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