Release Notes for the Catalyst 4900 Series Switch, Cisco IOS Release 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)SG7, 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 the Cisco IOS Release 15.0(2)SG on the Catalyst 4900 series switch (WS-C4928-10GE, WS-C4948, and WS-C4948-10GE).

To view the release notes for WS-C4900M, WS-C4948E, and WS-C4948E-F, see the URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_24730.html

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:

- Cisco IOS Software Packaging for the Cisco Catalyst 4900 Series Switch, page 2
- Cisco IOS Release Strategy for the Catalyst 4900 Series Switch, page 15

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

- System Requirements, page 16
- New and Changed Information, page 17
- Upgrading the System Software, page 18
- Limitations and Restrictions, page 31
- Caveats, page 38
- Troubleshooting, page 95
- Related Documentation, page 96
- Notices, page 98
- Obtaining Documentation and Submitting a Service Request, page 100

Cisco IOS Software Packaging for the Cisco Catalyst 4900 Series Switch

The Enterprise Services image supports all Cisco Catalyst 4500 Series software features based on Cisco IOS Software, including enhanced routing.

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

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. 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 4900 Series Switch, support for Network Edge Access Topology (NEAT) has been extended from IP Base to LAN Base and support for HSRPv2 for IPv6 has been extended from Enterprise Services to IP Base.

For more information about the Cisco Catalyst 4900 series switch, visit http://www.cisco.com/en/US/products/ps6021/index.html

Topics include:

- Feature Support on the LAN Base vs IP Base Images, page 2
- Unsupported Features, page 14
- Orderable Product Numbers, page 15

Feature Support on the LAN Base vs IP Base Images

Table 1 is a detailed list of features supported on Catalyst 4900 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 4900 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	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

Table 1 LAN Base/IP Base Image Support on the Catalyst 4900 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
Bidirectional PIM (IPv4 only)	No	Yes	Yes
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
Config File	Yes	Yes	Yes
Configuration Replace and Configuration Rollback	Yes	Yes	Yes
Configuration Rollback Confirmed Change	No	No	Yes
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

Table 1 LAN Base/IP Base Image Support on the Catalyst 4900 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
DHCP - DHCPv6 Relay Agent notification for Prefix Delegation	No	Yes	Yes
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 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 4900 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
Flex Link+(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	Yes
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	Yes
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 4900 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 Authentication	Yes	Yes	Yes
IEEE 802.1x Multi-Domain Authentication with Voice VLAN Assignment	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

Table 1 LAN Base/IP Base Image Support on the Catalyst 4900 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
IP Enhanced IGRP Route Authentication	No	No	Yes
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 Random Scheduler	No	No	Yes
IP SLAs Reaction Threshold	No	No	Yes
IP SLAs Responder	No	Yes	Yes
IP SLAs Sub-millisecond Accuracy Improvements	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

Table 1 LAN Base/IP Base Image Support on the Catalyst 4900 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
IP SLAs UDP Jitter Operation	No	No	Yes
IP SLAs VoIP Threshold Traps	No	No	Yes
IP Source Guard v4	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 4900 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
Layer 2 Protocol Tunneling (L2PT)	No	Yes	Yes
Layer 2 Traceroute	Yes	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
Network Time Protocol (NTP) master	Yes	Yes	Yes
No. of QoS Filters No. of Security ACE	Yes (4K entries)	Yes	Yes
No. of VLAN Support	2048	4096	Yes
NSF - BGP	No	No	Yes
NSF - EIGRP	No	No	Yes
NSF - OSPF v2	No	No	Yes
NSF/SSO (Nonstop Forwarding with Stateful Switchover)	No	No	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4900 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
On Demand Routing (ODR)	No	No	Yes
OSPF	No	Yes[2]	Yes
OSPF Flooding Reduction	No	Yes[2]	Yes
OSPF for Routed Access	No	Yes	Yes
OSPF Incremental Shortest Path First (i-SPF) Support	No	Yes[2]	Yes
OSPF Link State Database Overload Protection	No	Yes[2]	Yes
OSPF Not-So-Stubby Areas (NSSA)	No	Yes[2]	Yes
OSPF Packet Pacing	No	Yes[2]	Yes
OSPF Shortest Paths First Throttling	No	Yes[2]	Yes
OSPF Stub Router Advertisement	No	Yes[2]	Yes
OSPF Support for Fast Hellos	No	Yes[2]	Yes
OSPF Support for Link State Advertisement (LSA) Throttling	No	Yes[2]	Yes
OSPF Support for Multi-VRF on CE Routers	No	Yes[2]	Yes
OSPF Update Packet-Pacing Configurable Timers	No	Yes[2]	Yes
Out-of-band Management Port	Yes	Yes	Yes
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
Port Monitoring (interface Stats)	Yes	Yes	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4900 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
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	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
Service Advertisement Framework (SAF)	No	No	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4900 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
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 sessions)	Yes (8 bidirectional sessions)	Yes
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	Yes
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
VLAN Mapping (VLAN Translation)	Yes	Yes	Yes

Table 1 LAN Base/IP Base Image Support on the Catalyst 4900 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
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 Catalyst 4900M.
2. IP Base supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 200 dynamically learned routes.

Note With the LAN Base image, 10GbE uplinks are supported on the Catalyst 4948-10GE switch but not the Catalyst 4948 switch.

Unsupported Features

These features are not supported in Cisco IOS Release 15.0(2)SG for the 4900 series switches:

- The following MIBs:
  - cpmCPUMemoryUsed
  - cpmCPUMemoryFree
  - cpmCPUMemoryKernelReserved
  - cpmCPUMemoryLowest
  - cpmCPUMemoryUsedOvrflw
  - cpmCPUMemoryHCUsed
  - cpmCPUMemoryFreeOvrflw
  - cpmCPUMemoryHCFree
  - cpmCPUMemoryKernelReservedOvrflw
  - cpmCPUMemoryHCKernelReserved
  - cpmCPUMemoryLowestOvrflw
  - cpmCPUMemoryHCLowest
- The following ACL types:
  - Standard Xerox Network System (XNS) access list
  - Extended XNS access list
  - DECnet access list
  - Protocol type-code access list

- CEF Accounting
- Cisco IOS software IPX ACLs:
  - <1200-1299> IPX summary address access list
- ADSL and Dial access for IPv6
- AppleTalk EIGRP (use native AppleTalk routing instead)
- Bridge groups
- 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
- Lock and key
- NAT-PT for IPv6
- Netflow
- PBR with Multiple Tracking Options
- QoS for IPv6 (QoS for IPv6 traffic)
- Reflexive ACLs
- Routing IPv6 over an MPLS network
- Two-way community VLANs in private VLANs
- CFM CoS
- PBR with EOT
- Unicast RPF

Orderable Product Numbers

- S49ES-15002SG(=)—Cisco Catalyst 4900 IOS Enterprise Services w/o CRYPTO
- S49ESK9-15002SG—Cisco Catalyst 4900 IOS Enterprise Services SSH
- S49IPB-15002SG(=)—Cisco Catalyst 4900 IOS IP Base w/o CRYPTO
- S49IPBK9-15002SG(=)—Cisco Catalyst 4900 IOS IP Base SSH
- S49LB-15002SG(=)—Cisco Catalyst 4900 IOS LAN Base w/o CRYPTO
- S49LBK9-15002SG(=)—Cisco Catalyst 4900 IOS LAN Base SSH

Cisco IOS Release Strategy for the Catalyst 4900 Series Switch

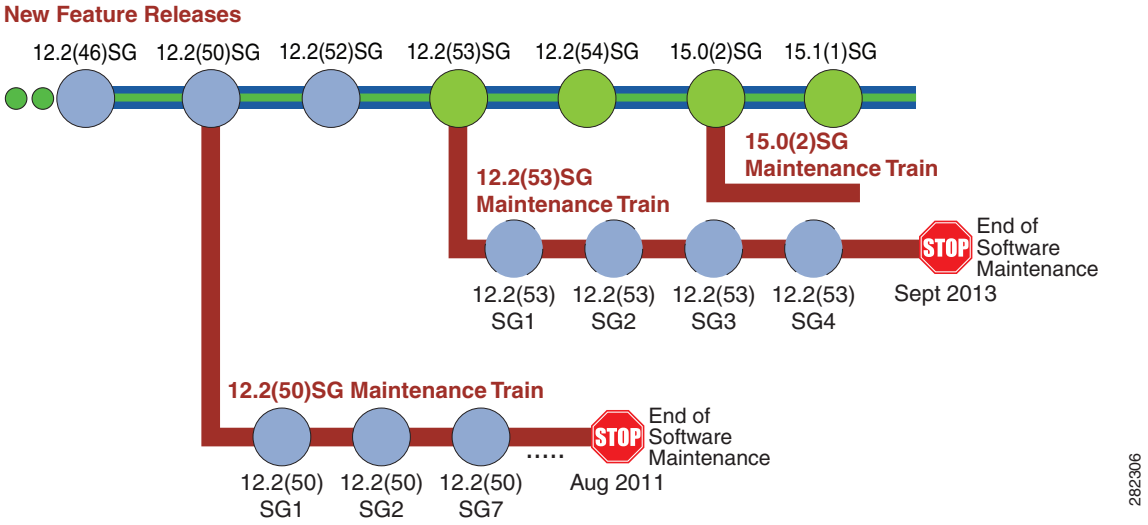
Customers with Catalyst 4900 series switches who need the latest hardware support and software features should migrate to Cisco IOS Release 15.0(2)SG. Cisco IOS Release 15.0(2)SG is the latest maintenance train base.

Cisco IOS Release 12.2(53)SG4 is the recommended release for customers who require a release with a maintenance train. The Cisco IOS Release 12.2(53)SG train includes support for OSPF for routed Access.

Cisco IOS Software Migration

Figure 1 displays the two active trains.

Figure 1 Software Release Strategy for the Catalyst 4900 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, page 16

Supported Hardware

This section describes the hardware supported on the Catalyst 4900 series switch.

For Catalyst 4900 series switch transceiver module compatibility information, see the url:

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

Table 2 briefly describes the Catalyst 4900 series switch product set.

Table 2 WS-4948 and WS-4948-10GE

Product Number (append with "=" for spares)	Product Description	Software Release
		Minimum
WS-X4948	48-port 10/100/1000 Catalyst 4948 switch, optional software image, optional power supplies, fan tray	12.2(20)EWA
WS-X4948-S	48-port 10/100/1000 Catalyst 4948 switch, SMI, one AC power supply, fan tray	12.2(20)EWA
WS-X4948-E	48-port 10/100/1000 Catalyst 4948 switch, EMI, one AC power supply, fan tray	12.2(20)EWA
WS-X4948-10GE	48-port 10/100/1000 2-10GE Catalyst 4948 switch, optional software image, optional power supplies, fan tray	12.2(25)EWA
WS-X4948-10GE-S	48-port 10/100/1000 2-10GE Catalyst 4948 switch, SMI, one AC power supply, fan tray	12.2(25)EWA
WS-X4948-10GE-E	48-port 10/100/1000 2-10GE Catalyst 4948 switch, EMI, one AC power supply, fan tray	12.2(25)EWA
WS-C4928-10GE	24 Gigabit Ethernet Small Form-Factor Pluggable (SFP) downlinks, 4 Gigabit Ethernet SFP uplinks, two 10 Gigabit Ethernet X2 uplinks, redundant field-replaceable AC and DC power supplies, fan tray with redundant fans, 1 rack unit (RU) form factor	12.2(46)SG

New and Changed Information

These sections describe the new and changed information for the Catalyst 4900 series switch running Cisco IOS software:

- New Hardware Features in Release 15.0(2)SG1, page 17
- New Software Features in Release 15.0(2)SG1, page 17
- New Hardware Features in Release 15.0(2)SG, page 18
- New Software Features in Release 15.0(2)SG, page 18

New Hardware Features in Release 15.0(2)SG1

Release 15.0(2)SG1 provides no new hardware on the Catalyst 4900 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 4900 series switch:

- 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 hardware on the Catalyst 4900 series switch:

- SFP-10-ER

New Software Features in Release 15.0(2)SG

Release 15.0(2)SG provides the following new software features on the Catalyst 4900 series switch:

- 2-way Community Private VLANs ("Configuring Private VLANs" chapter)
- Call Home message using dedicated interface (“Configuring Call Home” chapter)
- Critical Authorization for Voice and Data (“Configuring 802.1X Port-Based Authentication 802.1X” chapter)
- Duplication Location Reporting Issue

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

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

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, the following tables list the recommended ROMMON release.

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 3 Catalyst 4900 Series Switches, Recommended ROMMON Release, and Promupgrade Programs

Switching Module	Minimum ROMMON Release	Promupgrade Program
WS-X4948	12.2(20r)EW	cat4500-ios-promupgrade-122_31r_SGA4
WS-X4948-10GE	12.2(25r)EWA	cat4500-ios-promupgrade-122_31r_SGA4
WS-C4928-10GE	12.2(31r)SGA2	cat4500-ios-promupgrade-122_31r_SGA4

The following sections describe how to upgrade your switch software:

- Upgrading the ROMMON from the Console, page 19
- Upgrading the ROMMON Remotely Using Telnet, page 22
- Upgrading the Cisco IOS Software, page 27

Upgrading the 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(31r)SGA4 and Cisco IOS Release 12.2(25)EWA. For other releases, replace the ROMMON release and Cisco IOS software release with the appropriate releases and filenames.

Follow this procedure to upgrade your supervisor engine ROMMON:

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

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-ios-promupgrade-122_31r_SGA1SGA4 program from Cisco.com, and place it on a TFTP server in a directory that is accessible from the switch that will be upgraded.

The cat4500-ios-promupgrade-122_31r_SGA1SGA4 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 issue the **squeeze bootflash:** command to reclaim the space.

Step 4 Download the cat4500-ios-promupgrade-122_31r_SGA1SGA4 program into Flash memory using the copy tftp command.

The following example shows how to download the PROM upgrade image cat4500-ios-promupgrade-122_31r_SGA1 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-ios-promupgrade-122_31r_SGA1SGA4]?
```

```
Destination filename [cat4500-ios-promupgrade-122_31r_SGA1SGA4]?
Accessing tftp://172.20.58.78/cat4500-ios-promupgrade-122_31r_SGA1SGA4...
Loading cat4500-ios-promupgrade-122_31r_SGA1SGA4 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
[OK - 455620 bytes]

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

Step 5 Enter the **reload** command to reset the switch, press **Ctrl-C** to stop the boot process, and re-enter ROMMON.

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

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

2d11h: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command
.
************************************************************
 *                                                          *
 * Welcome to Rom Monitor for WS-C4948-10GE System.         *
 * Copyright (c) 1999-2005 by Cisco Systems, Inc.           *
 * All rights reserved.                                     *
 *                                                          *
 ************************************************************

 Rom Monitor Program Version 12.2(25r)EWA
 Supervisor: WS-C4948-10GE  Chassis: WS-C4948
 Hardware Revisions - Board: 8.3 CPLD Gill: 17

 MAC Address  : 00-0b-fc-ff-3b-ff
 IP Address   : 10.5.43.225
 Netmask      : 255.255.255.0
 Gateway      : 10.5.43.1
 TftpServer   : 10.5.5.5

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

 Type control-C to prevent autobooting.
 . .
 Autoboot cancelled......... please wait!!!

 Autoboot cancelled......... please wait!!!
rommon 1 > [interrupt]
```

Step 6 Run the PROM upgrade program by entering this command:**?boot bootflash:cat4500-ios-promupgrade-122_31r_SGA1SGA4**

Caution 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 output from a successful upgrade, followed by a system reset:

```
rommon 2 > bootflash:cat4500-ios-promupgrade-122_31r_SGA1SGA4


 ************************************************************
 *                                                          *
 * Rom Monitor Upgrade Utility For WS-C4948-10GE System     *
```

```
* This upgrades flash Rom Monitor image to the latest    *
*                                                        *
* Copyright (c) 1997-2005 by Cisco Systems, Inc.         *
* All rights reserved.                                   *
*                                                        *
**********************************************************

Image size = 1024.0 KBytes

Maximum allowed size = 1048576 KBytes


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

Beginning erase of 0x100000 bytes at offset 0x3e00000...  Done!

Beginning write of prom  (0x100000 bytes at offset 0x3e00000)...

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

Verifying...

Success! The prom has been upgraded successfully.
System will reset itself and reboot within few seconds....
```

Step 7 Boot the Cisco IOS software image, and enter the **show version** command to verify that ROMMON has been upgraded to 12.2(31r)SGA4.

Step 8 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 cat4500-ios-promupgrade-122_31r_SGA1SGA4 image from bootflash and reclaim unused space:

```
Switch# delete bootflash:cat4500-ios-promupgrade-122_31r_SGA1SGA4
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 9 Use the **show version** command to verify that the ROMMON has been upgraded

```
Switch# show version
Cisco IOS Software, Catalyst 4900 L3 Switch Software (cat4500-IPBASE-M), Version
12.2(25)EWA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 17-Aug-05 17:09 by alnguyen
Image text-base: 0x10000000, data-base: 0x11269914

ROM: 12.2(31r)SGA4
Pod Revision 0, Force Revision 31, Tie Revision 17

Switch uptime is 1 minute
System returned to ROM by reload
System image file is "bootflash:cat4500-ipbase-mz.122-25.EWA"

cisco WS-C4948-10GE (MPC8540) processor (revision 3) with 262144K bytes of memory.
Processor board ID 0
MPC8540 CPU at 667Mhz, Fixed Module
```

```
Last reset from Reload
1 Virtual Ethernet interface
48 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.

Configuration register is 0x2

Switch#
```

The ROMMON has now been upgraded.

See the "Upgrading the Cisco IOS Software" section on page 27 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the 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(31r)SGA4. 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 on the following section, use the PROM upgrade version cat4500-ios-promupgrade-122_31r_SGA1SGA4.

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 cat4500-ios-promupgrade-122_31r_SGA1SGA4 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-ios-promupgrade-122_31r_SGA1SGA4 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 issue the **squeeze bootflash:** command to reclaim the space.

Step 4 Download the cat4500-ios-promupgrade-122_31r_SGA1SGA4 program into Flash memory using the **copy tftp** command.

The following example shows how to download the PROM upgrade image cat4500-ios-promupgrade-122_31r_SGA1SGA4 from the remote host 10.5.5.5 to bootflash:

```
Switch# copy tftp: bootflash:
Address or name of remote host [10.5.5.5]?
Source filename [cat4500-ios-promupgrade-122_31r_SGA1SGA4]?
/tftpboot/pjose/cat4500-ios-promupgrade-122_31r_SGA1SGA4
```

```
Destination filename [cat4500-ios-promupgrade-122_31r_SGA1SGA4]?
Accessing tftp://10.5.5.5//tftpboot/pjose/cat4500-ios-promupgrade-122_31r_SGA1SGA4...
Loading /tftpboot/pjose/cat4500-ios-promupgrade-122_31r_SGA1SGA4 from 10.5.5.5 (via G
igabitEthernet1/1): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1244496 bytes]

1244496 bytes copied in 9.484 secs (131221 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 cat4500-ios-promupgrade-122_31r_SGA1SGA4 from bootflash:

```
Switch# configure terminal
Switch(config)# no boot system flash
bootflash:cat4500-ios-promupgrade-122_31r_SGA1SGA4
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(31r)SGA4EWA. After the ROMMON upgrade is complete, the supervisor engine will boot
Cisco IOS software Release 12.2(25)EWA.

config-register to 0x0102

Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4500-ios-promupgrade-122_31r_SGA1SGA4
Switch(config)# boot system flash bootflash:cat4500-ipbase-mz.122-25.EWA
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:cat4500-ios-promupgrade-122_31r_SGA1SGA4,1;bootflash:cat4500-ipbase-mz.122-25.EW
A
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 will be 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]

00:00:36: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command



************************************************************
 *                                                          *
 * Welcome to Rom Monitor for WS-C4948-10GE System.         *
 * Copyright (c) 1999-2005 by Cisco Systems, Inc.           *
 * All rights reserved.                                     *
 *                                                          *
 ************************************************************

 Rom Monitor Program Version 12.2(25r)EWA
 Supervisor: WS-C4948-10GE  Chassis: WS-C4948
 Hardware Revisions - Board: 8.0 CPLD : 17 FPGA : 0

 MAC Address  : 00-0b-fc-ff-3b-ff
 IP Address   : 10.5.43.225
 Netmask      : 255.255.255.0
 Gateway      : 10.5.43.1
 TftpServer   : 10.5.5.5

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

 Type control-C to prevent autobooting.
 . . . . .
 ******** The system will autoboot now ********

 config-register = 0x102
 Autobooting using BOOT variable specified file.....
 Current BOOT file is --- bootflash:cat4500-ios-promupgrade-122_31r_SGA1SGA4

************************************************************
 *                                                          *
 * Rom Monitor Upgrade Utility For WS-C4948-10GE System     *
 * This upgrades flash Rom Monitor image to the latest      *
 *                                                          *
 * Copyright (c) 1997-2005 by Cisco Systems, Inc.           *
 * All rights reserved.                                     *
```

```
 *                                                          *
 ************************************************************
 Image size = 1024.0 KBytes
 Maximum allowed size = 1048576 KBytes

Upgrading your PROM... DO NOT RESET the system
 unless instructed or upgrade of PROM will fail !!!
 Beginning erase of 0x100000 bytes at offset 0x3e00000...  Done!
 Beginning write of prom  (0x100000 bytes at offset 0x3e00000)...
 This could take as little as 30 seconds or up to 2 minutes.
 Please DO NOT RESET!
 Verifying...
 Success! The prom has been upgraded successfully.
 System will reset itself and reboot within few seconds....

****
 (output truncated)
 . . . . .
 ******** The system will autoboot now ********

 config-register = 0x102
 Autobooting using BOOT variable specified file.....
 Current BOOT file is --- bootflash:cat4500-ipbase-mz.122-25.EWA
Rommon reg: 0x00004180
############
(output truncated)
Exiting to ios...
Rommon reg: 0x00000180
################################
              Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco IOS Software, Catalyst 4900 L3 Switch Software (cat4500-IPBASE-M), Version
12.2(25)EWA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 17-Aug-05 17:09 by alnguyen
Image text-base: 0x10000000, data-base: 0x11269914
cisco WS-C4948-10GE (MPC8540) processor (revision 3) with 262144K bytes of memory.

Processor board ID 0
MPC8540 CPU at 667Mhz, Fixed Module
Last reset from Reload
1 Virtual Ethernet interface
48 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.
Uncompressed configuration from 1171 bytes to 2726 bytes

Press RETURN to get started!

Switch> enable
Switch#
```

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:cat4500-ios-promupgrade-122_31r_SGA1SGA4
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 IOS Software, Catalyst 4900 L3 Switch Software (cat4500-IPBASE-M), Version
12.2(25)EWA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 17-Aug-05 17:09 by alnguyen
Image text-base: 0x10000000, data-base: 0x11269914

ROM: 12.2(31r)SGA4
Pod Revision 0, Force Revision 31, Tie Revision 17

Switch uptime is 0 minutes
System returned to ROM by reload
System image file is "bootflash:cat4500-ipbase-mz.122-25.EWA"

cisco WS-C4948-10GE (MPC8540) processor (revision 3) with 262144K bytes of memory.
Processor board ID 0

MPC8540 CPU at 667Mhz, Fixed Module
Last reset from Reload
1 Virtual Ethernet interface
48 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.

Configuration register is 0x102

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 cat4500-ios-promupgrade-122_31r_SGA1SGA4 image from bootflash and reclaim unused space:

```
Switch# delete bootflash:cat4500-ios-promupgrade-122_31r_SGA1SGA4
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:cat4500-ipbase-mz.122-25.EWA,12;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
```

```
Switch#
```

The ROMMON has now been upgraded.

See the "Upgrading the Cisco IOS Software" section on page 27 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 4900 series switch, use this procedure:

Step 1 Download Cisco IOS Release 12.2(25)EWA from Cisco.com, and place the image on a TFTP server in a directory that is accessible from the supervisor engine that will be 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.

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 cat4500-ipbase-mz.122-25.EWA 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-ipbase-mz.122_25.EWA]?
Destination filename [cat4500-ipbase-mz.122-25.EWA]?
Accessing tftp://172.20.58.78/cat4500-ipbase-mz.122-25.EWA...
Loading cat4500-ipbase-mz.122-25.EWA 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 cat4500-ipbase-mz.122-25.EWA 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:cat4500-ipbase-mz.122_25.EWA
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 cat4500-ipbase-mz.122-25.EWA image to the BOOT variable:

```
Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4500-ipbase-mz.122_25.EWA
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 No 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

System configuration has been modified. Save? [yes/no]: yes
Building configuration...
```

```
Compressed configuration from 2668 bytes to 1127 bytes[OK]
Proceed with reload? [confirm]

00:02:11: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Comm
and.

**********************************************************
 *                                                        *
 * Welcome to Rom Monitor for WS-C4948-10GE System.       *
 * Copyright (c) 1999-2005 by Cisco Systems, Inc.         *
 * All rights reserved.                                   *
 *                                                        *
 **********************************************************

 Rom Monitor Program Version 12.2(25r)EWA
 Supervisor: WS-C4948-10GE  Chassis: WS-C4948
 Hardware Revisions - Board: 8.3 CPLD Gill: 17


 MAC Address  : 00-0b-fc-ff-3b-ff
 IP Address   : 10.5.43.225
 Netmask      : 255.255.255.0
 Gateway      : 10.5.43.1
 TftpServer   : 10.5.5.5


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


 Type control-C to prevent autobooting.
 . . . . .

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


 config-register = 0x2102
 Autobooting using BOOT variable specified file.....

 Current BOOT file is --- bootflash:cat4500-ipbase-mz.122-25.EWA

Rommon reg: 0x00004180
############
k2diags version 5.0.1_e

prod: WS-C4948-10GE  part: 0  serial: 0


Power-on-self-test for Module 1:  WS-C4948-10GE
 Port/Test Status: (. = Pass, F = Fail, U = Untested)

Cpu Subsystem Tests ...
seeprom: . temperature_sensor: .

Port Traffic: L2 Serdes Loopback ...
 0: .  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
62: . 63: .


Port Traffic: L2 Asic Loopback ...
 0: .  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
```

```
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
62: . 63: .


Port Traffic: L3 Asic Loopback ...
 0: .  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
62: . 63: .


Switch Subsystem Memory ...
 1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: . 12: .
13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: . 24: .
25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: . 36: .
37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: . 48: .
49: . 50: . 51: .


Front Panel Ports ...
 1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: . 12: .
13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: . 24: .
25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: . 36: .
37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: . 48: .


Module 1 Passed


Exiting to ios...

Rommon reg: 0x00000180
################################
              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software, Catalyst 4900 L3 Switch Software (cat4500-IPBASE-M), Version
 12.2(25)EWA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 17-Aug-05 17:09 by alnguyen
Image text-base: 0x10000000, data-base: 0x11269914
```

```
#    #    ##    #####   #    #    #    #    #   ####
#    #   #  #   #    #  ##   #    #    ##   #  #    #
#    #  #    #  #    #  # #  #    #    # #  #  #
# ## #  ######  #####   #  # #    #    #  # #  #  ###
##  ##  #    #  #   #   #   ##    #    #   ##  #    #
#    #  #    #  #    #  #    #    #    #    #   ####

The following environment variable(s) are set.  Setting these
environment variables may cause the system to behave unpredictably.
        "DontShipAllowChassisSimulation"
        "gdbEnable"
Use 'clear platform environment variable unsupported' to clear these variables.

cisco WS-C4948-10GE (MPC8540) processor (revision 3) with 262144K bytes of memor
y.
Processor board ID 0
MPC8540 CPU at 667Mhz, Fixed Module
Last reset from Reload
1 Virtual Ethernet interface
48 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.

Uncompressed configuration from 1127 bytes to 2668 bytes

Press RETURN to get started!

00:00:06: %C4K_IOSMODPORTMAN-4-POWERSUPPLYBAD: Power supply 2 has failed or been
 turned off
00:00:06: %C4K_IOSMODPORTMAN-4-POWERSUPPLYFANBAD: Fan of power supply 2 has fail
ed
00:00:15: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
00:00:15: %C4K_IOSMODPORTMAN-6-MODULEONLINE: Module 1 (WS-C4948-10GE S/N: 0 Hw:
0.3) is online
00:00:16: %SYS-5-CONFIG_I: Configured from memory by console
00:00:16: %SYS-5-RESTART: System restarted --
Cisco IOS Software, Catalyst 4900 L3 Switch Software (cat4500-IPBASE-M), Version
 12.2(25)EWA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 17-Aug-05 17:09 by alnguyen
Switch>
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 4900 series switch.

- For IP Unnumbered, 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 ACLis not supported on “Classic” supervisors. However, WCCP redirect ACLs are supported on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M and Catalyst 4948E from Cisco IOS 15.0(2)SG onwards and on Supervisor Engine 7-E, Supervisor Engine 7L-E, and Catalyst 4500X from Cisco IOS XE 3.3.0(SG) onwards.
- 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 PBR, the following are not supported:
  - Matching cannot be performed on packet lengths
  - IP precedence, TOS, and QoS group are fixed
  - ACL or route-map statistics cannot be updated
- IGRP not supported (use EIGRP, instead).
- IP classful routing is not supported; do not use the **no ip classless** command; it will have no effect, as only classless routing is supported. The command **ip classless** is not supported as classless routing is enabled by default.
- 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 95 for details on alternatives.
- 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 sample output of the **show standby GigabitEthernet1/1** command:

  ```
  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: Since the problem is caused by mismatched MTUs, the solution is to change the MTU on either router to match the neighbor's MTU.

- The Ethernet management port on the supervisor module is active in ROMMON mode only.
- If an original packet is dropped due to transmit queue shaping and/or sharing configurations, a SPAN packet copy can still be transmitted on the SPAN port.
- All software releases support a maximum of 32,768 IGMP snooping group entries.
- Use the **no ip unreachables** command on all interfaces with ACLs configured for performance reasons.
- 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.

  Workaround: Verify whether or not the Neighbor discovery cache has an entry, separate from regular troubleshooting areas of IPv6 address configurations and other configurations.

- 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 will be lost.
- By default, IPv6 is not enabled. To route IPv6, you must issue 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 (once 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.
- The maximum number of unique private VLAN pairs supported by the **switchport private-vlan mapping trunk** command above is 1000. 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.
- While configuring PVLAN promiscuous trunk ports, the maximum number of mappings is 500 primary VLANs to 500 secondary VLANs.
- 802.1X inaccessible authentication bypass feature is not supported with NAC LAN port IP feature.
- Changes to the console speed in "line console 0" configuration mode do not impact console speed in ROMMON mode. To apply the same console speed in ROMMON mode, use the "confreg" ROMMON utility and change ROMMON console speed.
- If a Catalyst 4900 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, check that there is network connectivity between the switch and the ACS. You should also check 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. Executing 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)
- IPSG for Static Hosts basically 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 (e.g. 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. Rather, 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 using Port Security with Multi Domain Authentication (MDA) on an interface:
  - You must allow for at least 3 MAC addresses to access the switch: 2 for the phone (the MAC address of a phone gets registered to the Data domain and Voice domain), and one for the PC.
  - The data and voice VLAN IDs must 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 hit 100 per cent if there are a large number of hosts to learn. The CPU usage will drop once 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 are displayed in the device tracking table as INACTIVE.
  - Autostate SVI does not work on EtherChannel.
- After the fix for CSCsg08775, a GARP ACL entry is no longer part of the Static CAM area, but there is still a system-defined GARP class in Control Plane Policing (CPP). CPP is a macro with many CLIs and the GARP class creation CLI has been removed.
- When ipv6 is enabled on an interface via any CLI, it is possible to see the following message:

  ```
  % Hardware MTU table exhausted
  ```

  In such a scenario, the ipv6 MTU value programmed in hardware will be different from the ipv6 interface MTU value. This will happen if there is no room in the hw MTU table to store additional values.

You must free up some space in the table by unconfiguring some unused MTU values and subsequently disable/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, issue 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 only 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 will reject all the IP traffic from that interface.

Note The issue above also applies to IPSG with Static Hosts on a PVLAN Host port.

- Management port does not support *non-VRF* aware features.
- When you enter the **permit any any ?** command you will observe the **octal** option, which is unsupported in Cisco IOS Release 12.2(52)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 4900 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.
- After upgrading to Cisco IOS 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.

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

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.
- 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

- 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.

- 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.

Caveats

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

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

http://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 4 Resolved Caveats in IOS Release 15.0(2)SG11

Bug ID	Headline
CSCts66733	Crash @ tftp_server
CSCup90532	memory corruption crash related to DNS
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

Table 4 Resolved Caveats in IOS Release 15.0(2)SG11

Bug ID	Headline
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.
CSCvb21904	4948E: Platform command in config mode are hidden.

Open Caveats in 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 issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  – If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.

  – If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then 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 support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. 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 configure **qos account layer2 encapsulation**.

  Workaround: None. CSCsg58526

- When hardcoded 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 impact performance.

Workaround: Issue 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 is displayed and the port is not able to handle traffic.

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

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with HWCOPP (HW Control Plane Policing).

  Workaround: None. CSCso93282

- An IP unnumbered configuration is lost after a reload.

  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 such that during bootup, the router port is created first.

  CSCsq63051

- In SSO mode, when a port-channel is created, deleted, and re-created 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 portchannel, create a new channel. (CSCsr00333)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on 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

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

  Workaround: For VTP database propagation, configure ISL/dot1q trunk port. CSCsu43445

- 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 VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS. Specifically, 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

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Workaround: None.

  Despite the different default value, you can configure any value in the time range. 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 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 a NEAT configuration on an ASW (Catalyst 4500 series switch) connected to an SSW (Catalyst 3750 series switch) serving as a root bridge and with redundant links between ASW and SSW, the following occur:
  - STP does not stabilize.
  - The SVI (network) is unreachable. If an SVI exists on the ASW, because of the STP flap in the setup as well as the CISP operations, the SVI MAC configuration on the ASW is incorrect.

Workaround: Configure the ASW or any other switch upstream as the root-bridge for all the VLANs. CSCtg71030

- 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

- 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

- 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 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

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

  Workaround: None. CSCtx95359

Resolved Caveats in Cisco IOS 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 in Cisco IOS Release 15.0(2)SG9

This section lists the resolved caveats in 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 "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 "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 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

- 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

- 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

- 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

- 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.

  Workarounds:

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

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

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

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

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

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

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

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

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

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

  CSCum12826

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

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

48 Gigabit Ethernet 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

- With the following topology, one Gig traffic with any odd size packets are dropped if egress is in uplink ports of 4948-E at line rate

IXIA(01/02) ------ (Gi1/2)C4948E(Ten1/49) ------ (05/02)IXIA

It is more likely that you will see drops with smaller, randomly sized packets, where COS is set to 0.

Workaround: None. CSCun22906

- 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

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

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

  Workaround: None. CSCuo89407

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

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

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
- If the ACL TCAM space is exhausted and traffic begins to punt, CPU remains high after the ACL [TCAM] size is reduced.

  Workaround: Reconfigure ACLs on all affected interfaces or reload the switch. CSCuf93866
- High amounts of multicast or replicated SPAN traffic cause a switch to crash with 'System returned to ROM by abort at PC 0x0' in the output of the **show version** command. Crashdump reports an "IPP PRM pktParityInt interrupt" error followed by a crash, which may indicate a corrupted block redzone.

  To see a SPAN-induced crash, SPAN destination ports must receive pause frames from the remote side of the SPAN destination port.

  Catalyst 4900M, Catalyst 4948E, Supervisor Engine 6-E, and Supervisor Engine 6L-E are impacted.

  Workaround: If the problem is triggered by pause frames from remote SPAN destination ports, disable flow control on those ports.

  Later IOS releases have resolved this bug. CSCue11730

Open Caveats in Cisco IOS Release 15.0(2)SG7

This section lists the open caveats in Cisco IOS Release 15.0(2)SG7:

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then 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 support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

Workaround: Re-connect. 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 configure **qos account layer2 encapsulation**.

  Workaround: None. CSCsg58526

- When hardcoded 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 impact performance.

  Workaround: Issue 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 is displayed and the port is not able to handle traffic.

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

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with HWCOPP (HW Control Plane Policing).

  Workaround: None. CSCso93282

- An IP unnumbered configuration is lost after a reload.

  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 such that during bootup, the router port is created first.

  CSCsq63051

- In SSO mode, when a port-channel is created, deleted, and re-created 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 portchannel, create a new channel. (CSCsr00333)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on 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

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

  Workaround: For VTP database propagation, configure ISL/dot1q trunk port. CSCsu43445

- 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 VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS. Specifically, 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

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Workaround: None.

Despite the different default value, you can configure any value in the time range. 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 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 a NEAT configuration on an ASW (Catalyst 4500 series switch) connected to an SSW (Catalyst 3750 series switch) serving as a root bridge and with redundant links between ASW and SSW, the following occur:
  - STP does not stabilize.
  - The SVI (network) is unreachable. If an SVI exists on the ASW, because of the STP flap in the setup as well as the CISP operations, the SVI MAC configuration on the ASW is incorrect.

  Workaround: Configure the ASW or any other switch upstream as the root-bridge for all the VLANs. CSCtg71030

- 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 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

- 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

- 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 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

- 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 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

- If the ACL TCAM space is exhausted and traffic begins to punt, CPU remains high after the ACL [TCAM] size is reduced.

Workaround: Reconfigure ACLs on all affected interfaces or reload the switch.

CSCuf93866

Resolved Caveats in Cisco IOS Release 15.0(2)SG7

This section lists the resolved caveats in Release 15.0(2)SG7:

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

  Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports. CSCud05521

Open Caveats in Cisco IOS Release 15.0(2)SG6

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

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then 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 support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. 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 configure **qos account layer2 encapsulation**.

  Workaround: None. CSCsg58526
- When hardcoded 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 impact performance.

  Workaround: Issue 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 is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. CSCse34693
- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with HWCOPP (HW Control Plane Policing).

  Workaround: None. CSCso93282
- An IP unnumbered configuration is lost after a reload.

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 such that during bootup, the router port is created first.

CSCsq63051

- In SSO mode, when a port-channel is created, deleted, and re-created 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 portchannel, create a new channel. (CSCsr00333)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on 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

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

  Workaround: For VTP database propagation, configure ISL/dot1q trunk port. CSCsu43445

- 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 VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS. Specifically, 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

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Workaround: None.

  Despite the different default value, you can configure any value in the time range. 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 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 a NEAT configuration on an ASW (Catalyst 4500 series switch) connected to an SSW (Catalyst 3750 series switch) serving as a root bridge and with redundant links between ASW and SSW, the following occur:

  - STP does not stabilize.
  - The SVI (network) is unreachable. If an SVI exists on the ASW, because of the STP flap in the setup as well as the CISP operations, the SVI MAC configuration on the ASW is incorrect.

  Workaround: Configure the ASW or any other switch upstream as the root-bridge for all the VLANs. CSCtg71030

- 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 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

- 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

- 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 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

- 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

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

  Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports. CSCud05521

- 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
- If the ACL TCAM space is exhausted and traffic begins to punt, CPU remains high after the ACL [TCAM] size is reduced.

  Workaround: Reconfigure ACLs on all affected interfaces or reload the switch.

  CSCuf93866

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 AC156241000000670001BC9
  ```

  provided the following conditions apply:
  - A switchport is configured with the following:

authentication event server dead action authorize

authenticaton event server alive action reinitalize

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

The RADIUS server becomes available again, and the IAB-authorized port transitions to another state.

Workaround: None. CSCtx61557

Open Caveats in Cisco IOS Release 15.0(2)SG5

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

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  – If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  – If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then 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 support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. 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 configure **qos account layer2 encapsulation**.

  Workaround: None. CSCsg58526
- When hardcoded 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 impact performance.

  Workaround: Issue 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 is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. CSCse34693
- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with HWCOPP (HW Control Plane Policing).

  Workaround: None. CSCso93282
- An IP unnumbered configuration is lost after a reload.

  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 such that during bootup, the router port is created first.

  CSCsq63051

- In SSO mode, when a port-channel is created, deleted, and re-created 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 portchannel, create a new channel. (CSCsr00333)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on 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

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

  Workaround: For VTP database propagation, configure ISL/dot1q trunk port. CSCsu43445

- 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 VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS. Specifically, 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

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Workaround: None.

  Despite the different default value, you can configure any value in the time range. 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 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 a NEAT configuration on an ASW (Catalyst 4500 series switch) connected to an SSW (Catalyst 3750 series switch) serving as a root bridge and with redundant links between ASW and SSW, the following occur:
  - STP does not stabilize.
  - The SVI (network) is unreachable. If an SVI exists on the ASW, because of the STP flap in the setup as well as the CISP operations, the SVI MAC configuration on the ASW is incorrect.

  Workaround: Configure the ASW or any other switch upstream as the root-bridge for all the VLANs. CSCtg71030

- 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 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

- 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

- 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 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

- 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

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

  Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports. CSCud05521

- 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
- If the ACL TCAM space is exhausted and traffic begins to punt, CPU remains high after the ACL [TCAM] size is reduced.

  Workaround: Reconfigure ACLs on all affected interfaces or reload the switch.

  CSCuf93866

Resolved Caveats in Cisco IOS Release 15.0(2)SG5

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

- 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 in Cisco IOS Release 15.0(2)SG4

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

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then 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 support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. 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 configure **qos account layer2 encapsulation**.

  Workaround: None. CSCsg58526
- When hardcoded 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 impact performance.

  Workaround: Issue 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 is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. CSCse34693
- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with HWCOPP (HW Control Plane Policing).

  Workaround: None. CSCso93282
- An IP unnumbered configuration is lost after a reload.

  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 such that during bootup, the router port is created first.

  CSCsq63051
- In SSO mode, when a port-channel is created, deleted, and re-created 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 portchannel, create a new channel. (CSCsr00333)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on 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

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

  Workaround: For VTP database propagation, configure ISL/dot1q trunk port. CSCsu43445

- 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 VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS. Specifically, 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

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Workaround: None.

  Despite the different default value, you can configure any value in the time range. 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 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 a NEAT configuration on an ASW (Catalyst 4500 series switch) connected to an SSW (Catalyst 3750 series switch) serving as a root bridge and with redundant links between ASW and SSW, the following occur:

  - STP does not stabilize.
  - The SVI (network) is unreachable. If an SVI exists on the ASW, because of the STP flap in the setup as well as the CISP operations, the SVI MAC configuration on the ASW is incorrect.

  Workaround: Configure the ASW or any other switch upstream as the root-bridge for all the VLANs. CSCtg71030

- 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 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

- 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

- 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 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

- 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

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

  Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports. CSCud05521

- 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

- If the ACL TCAM space is exhausted and traffic begins to punt, CPU remains high after the ACL [TCAM] size is reduced.

  Workaround: Reconfigure ACLs on all affected interfaces or reload the switch.

  CSCuf93866

Resolved Caveats in Cisco IOS Release 15.0(2)SG4

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

- 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 in Cisco IOS Release 15.0(2)SG3

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

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then 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 support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. 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 configure **qos account layer2 encapsulation**.

  Workaround: None. CSCsg58526

- When hardcoded 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 impact performance.

  Workaround: Issue 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 is displayed and the port is not able to handle traffic.

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

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with HWCOPP (HW Control Plane Policing).

  Workaround: None. CSCso93282

- An IP unnumbered configuration is lost after a reload.

  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 such that during bootup, the router port is created first.

  CSCsq63051

- In SSO mode, when a port-channel is created, deleted, and re-created 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 portchannel, create a new channel. (CSCsr00333)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on 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

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

  Workaround: For VTP database propagation, configure ISL/dot1q trunk port. CSCsu43445

- 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 VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS. Specifically, 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

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Workaround: None.

  Despite the different default value, you can configure any value in the time range. 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 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 a NEAT configuration on an ASW (Catalyst 4500 series switch) connected to an SSW (Catalyst 3750 series switch) serving as a root bridge and with redundant links between ASW and SSW, the following occur:
  - STP does not stabilize.
  - The SVI (network) is unreachable. If an SVI exists on the ASW, because of the STP flap in the setup as well as the CISP operations, the SVI MAC configuration on the ASW is incorrect.

  Workaround: Configure the ASW or any other switch upstream as the root-bridge for all the VLANs. CSCtg71030

- 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 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

- 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

- 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 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

- 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

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

  Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports. CSCud05521

- 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

- If the ACL TCAM space is exhausted and traffic begins to punt, CPU remains high after the ACL [TCAM] size is reduced.

  Workaround: Reconfigure ACLs on all affected interfaces or reload the switch.

  CSCuf93866

Resolved Caveats in Cisco IOS Release 15.0(2)SG3

These are the new resolved caveats in Cisco IOS Release 15.0(2)SG3 for Catalyst 4900 Series Switch:

- 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 in Cisco IOS Release 15.0(2)SG2

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

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then 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 support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. 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 configure **qos account layer2 encapsulation**.

  Workaround: None. CSCsg58526
- When hardcoded 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 impact performance.

  Workaround: Issue 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 is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. CSCse34693
- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with HWCOPP (HW Control Plane Policing).

  Workaround: None. CSCso93282
- An IP unnumbered configuration is lost after a reload.

  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 such that during bootup, the router port is created first.

  CSCsq63051
- In SSO mode, when a port-channel is created, deleted, and re-created 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 portchannel, create a new channel. (CSCsr00333)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on 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

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

  Workaround: For VTP database propagation, configure ISL/dot1q trunk port. CSCsu43445

- 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 VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS. Specifically, 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

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Workaround: None.

  Despite the different default value, you can configure any value in the time range. 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 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 a NEAT configuration on an ASW (Catalyst 4500 series switch) connected to an SSW (Catalyst 3750 series switch) serving as a root bridge and with redundant links between ASW and SSW, the following occur:

  – STP does not stabilize.

  – The SVI (network) is unreachable. If an SVI exists on the ASW, because of the STP flap in the setup as well as the CISP operations, the SVI MAC configuration on the ASW is incorrect.

  Workaround: Configure the ASW or any other switch upstream as the root-bridge for all the VLANs. CSCtg71030

- 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 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

- 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

- 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 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

- 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

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

  Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports. CSCud05521

- 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

- If the ACL TCAM space is exhausted and traffic begins to punt, CPU remains high after the ACL [TCAM] size is reduced.

  Workaround: Reconfigure ACLs on all affected interfaces or reload the switch.

  CSCuf93866

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

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

  Workaround:

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

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

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

  Workarounds:

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

- 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 in Cisco IOS Release 15.0(2)SG1

This section lists the open caveats in Cisco IOS Release 15.0(2)SG1:

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then 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 support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. 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 configure **qos account layer2 encapsulation**.

  Workaround: None. CSCsg58526

- When hardcoded 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 impact performance.

  Workaround: Issue 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 is displayed and the port is not able to handle traffic.

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

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with HWCOPP (HW Control Plane Policing).

  Workaround: None. CSCso93282

- An IP unnumbered configuration is lost after a reload.

  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 such that during bootup, the router port is created first.

  CSCsq63051

- In SSO mode, when a port-channel is created, deleted, and re-created 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 portchannel, create a new channel. CSCsr00333

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on 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

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

  Workaround: For VTP database propagation, configure ISL/dot1q trunk port. CSCsu43445

- 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 VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS. Specifically, 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

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Workaround: None.

  Despite the different default value, you can configure any value in the time range. 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 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 a NEAT configuration on an ASW (Catalyst 4500 series switch) connected to an SSW (Catalyst 3750 series switch) serving as a root bridge and with redundant links between ASW and SSW, the following occur:
  - STP does not stabilize.
  - The SVI (network) is unreachable. If an SVI exists on the ASW, because of the STP flap in the setup as well as the CISP operations, the SVI MAC configuration on the ASW is incorrect.

  Workaround: Configure the ASW or any other switch upstream as the root-bridge for all the VLANs. CSCtg71030

- 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 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

- 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

- 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 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 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

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

  Workaround:

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

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

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

  Workarounds:

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

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

- 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

- 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

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

  Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports. CSCud05521

- 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

- If the ACL TCAM space is exhausted and traffic begins to punt, CPU remains high after the ACL [TCAM] size is reduced.

  Workaround: Reconfigure ACLs on all affected interfaces or reload the switch.

  CSCuf93866

Resolved Caveats in Cisco IOS Release 15.0(2)SG1

This section lists the resolved caveats in Release 15.0(2)SG1:

- 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 is 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

- 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

- 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

Open Caveats in Cisco IOS Release 15.0(2)SG

This section lists the open caveats in Cisco IOS Release 15.0(2)SG:

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then 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 support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. 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 configure **qos account layer2 encapsulation**.

  Workaround: None. CSCsg58526
- When hardcoded 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 impact performance.

  Workaround: Issue 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 is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. CSCse34693
- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with HWCOPP (HW Control Plane Policing).

  Workaround: None. CSCso93282
- An IP unnumbered configuration is lost after a reload.

  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 such that during bootup, the router port is created first.

  CSCsq63051
- In SSO mode, when a port-channel is created, deleted, and re-created 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 portchannel, create a new channel. CSCsr00333

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on 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

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

  Workaround: For VTP database propagation, configure ISL/dot1q trunk port. CSCsu43445

- 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 VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS. Specifically, 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

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Workaround: None.

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

- When Fallback WebAuth and Multi-host is 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

- With a NEAT configuration on an ASW (Catalyst 4500 series switch) connected to an SSW (Catalyst 3750 series switch) serving as a root bridge and with redundant links between ASW and SSW, the following occur:
  - STP does not stabilize.
  - The SVI (network) is unreachable. If an SVI exists on the ASW, because of the STP flap in the setup as well as the CISP operations, the SVI MAC configuration on the ASW is incorrect.

  Workaround: Configure the ASW or any other switch upstream as the root-bridge for all the VLANs. CSCtg71030

- 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

- 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

- 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

- 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 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

- 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 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

- 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

- 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

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

  Workaround: None. CSCto72927

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

  Workaround:

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

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

- When 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

- 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

- 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

- 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

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

  Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports. CSCud05521

- 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

- If the ACL TCAM space is exhausted and traffic begins to punt, CPU remains high after the ACL [TCAM] size is reduced.

  Workaround: Reconfigure ACLs on all affected interfaces or reload the switch.

  CSCuf93866

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 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 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

Troubleshooting

These sections provide troubleshooting guidelines for the Catalyst 4900 family running IOS supervisor engines:

- Netbooting from the ROMMON, page 95
- Troubleshooting at the System Level, page 96
- Troubleshooting Modules, page 96
- Troubleshooting MIBs, page 96

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 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 **cat4500-is-mz** located on the TFTP server 172.16.1.8, enter the following command:

```
rommon 3> boot tftp://172.16.1.8/tftpboot/cat4500-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. The Ethernet Management port is inoperative in all Cisco IOS releases (Cisco IOS Release 12.2(20)EWA through Cisco IOS Release 12.2(31)SGA). An Ethernet cable plugged into the Ethernet port is active only in ROMMON mode.

Troubleshooting Modules

This section contains troubleshooting guidelines for the Catalyst 4900 series switch:

- 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 4900 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:

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

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

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

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

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

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

Original SSLeay License:

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

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

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

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

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

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

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

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

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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

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

Release Notes for the Catalyst 4900 Series Switch, Cisco IOS Release 15.0(2)SG