Release Notes for the Catalyst 4900M Series Switch and the Catalyst 4948E Ethernet Switch, Cisco IOS Release 15.1(1)SG

Current Release
IOS 15.1(1)SG2—November 1, 2012

Previous Release
IOS 15.1(1)SG1 and IOS 15.1(1)SG

These release notes describe the features, modifications, and caveats for Cisco IOS Release 15.1(1)SG on the Catalyst 4900M switch and the Catalyst 4948E Ethernet Switch.

Cisco Catalyst 4900M Series is a premium extension to the widely deployed Catalyst 4948 Series top of rack Ethernet switches for data center server racks. Optimized for ultimate deployment flexibility, the Catalyst 4900M Series can be deployed for 10/100/1000 server access with 1:1 uplink to downlink oversubscription, mix of 10/100/1000 and 10 Gigabit Ethernet servers or all 10 Gigabit Ethernet servers in the same rack. The Catalyst 4900M is a 320Gbps, 250Mpps, 2RU fixed configuration switch with 8 fixed wire speed X2 ports on the base unit and 2 optional half card slots for deployment flexibility and investment protection. Low latency, scalable buffer memory and high availability with 1+1 hot swappable AC or DC power supplies and field replaceable fans optimize the Catalyst 4900M for any size of data center.

With Cisco IOS Release 12.2(54)XO, we Cisco introduced the Catalyst® 4948E Ethernet Switch, which is the first Cisco Catalyst E-Series data center switch built from the start to deliver class-leading, full-featured server-access switching. The switch offers forty-eight 10/100/1000-Gbps RJ45 downlink ports and four 1/10 Gigabit Ethernet uplink ports and is designed to simplify data center architecture and operations by offering service provider-grade hardware and software in a one rack unit (1RU) form factor optimized for full-featured top-of-rack (ToR) data center deployments.

The Cisco Catalyst 4948E Ethernet Switch builds on the advanced technology of the Cisco Catalyst 4948 Switches, the most deployed ToR switch in the industry, with more than 10 million ports deployed worldwide. The Cisco Catalyst E-Series doubles the uplink bandwidth and offers true front-to-back airflow with no side or top venting. Stringent airflow management reduces data center operating costs by providing strict hot-aisle and cold-aisle isolation. Exceptional reliability and serviceability are delivered with optional internal AC and DC 1+1 hot-swappable power supplies and a hot-swappable fan tray with redundant fans.

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

For more information on Catalyst 4900M and Catalyst 4948E Ethernet Switch, visit: http://www.cisco.com/en/US/products/ps6021/index.html.

Note Although this release note and those for Catalyst 4500 Series Switch, the Catalyst 4900 Series Switch, the Catalyst ME 4900 Switch, are unique, they each refer to the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide.*

Contents

This publication consists of these sections:

Cisco IOS Software Packaging

The Enterprise Services image supports Cisco Catalyst 4948E Ethernet Switch and Cisco Catalyst 4900M Series software features based on Cisco IOS Software 15.1(1)SG, including enhanced routing. BGP capability is included in the Enterprises Services package.

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

The LAN Base image complements the existing IP Base and Enterprise Services images. It is focused on customer access and Layer 2 requirements and therefore many of the IP Base features are not required. The IP upgrade image is available if at a later date you require some of those features. The Cisco Catalyst 4900M Switch Series only supports the IP Base and Enterprise Services images.

Starting with Cisco IOS Release 15.0(2)SG, on Catalyst 4900M and Catalyst 4948E, support for NEAT feature has been extended from IP Base to LAN Base and support for HSRP v2 IPV6 has been extended from Enterprise Services to IP Base.

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

Note The default image for WS-C4948E is LAN Base.

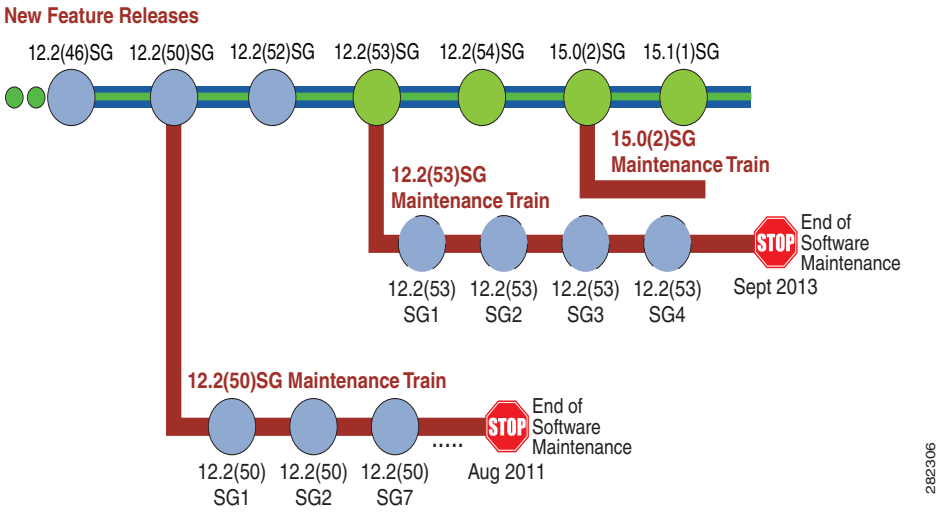
Cisco IOS Release Strategy

Customers with Catalyst 4948E Ethernet Switch and Catalyst 4900M series switches who need the latest hardware support and software features should migrate to Cisco IOS Release 15.1(1)SG.

The Catalyst 4900M Series Switch have has two maintenance trains: 12.2(53)SGx and 15.0(2)SGx. The Catalyst 4948E has one maintenance train: 15.0(2)SGx. Cisco IOS Release 15.0(2)SGx is the latest maintenance train. Figure 1 displays the two active trains, 12.2(53)SG and 15.0(2)SG.

Note Support for the Catalyst 4900M platform was introduced in 12.2(40)XO. Support for the Catalyst 4948E platform was introduced in 12.2(54)XO.

Figure 1 Software Release Strategy for the Catalyst 4900M Series Switch



Support

Support for Cisco IOS Software Release 15.1(1)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 on the Catalyst 4948E Ethernet Switch and Catalyst 4900M Series Switch:

Supported Hardware

For details on Catalyst 4900, 4948E, and 4948E-F switch transceiver module compatibility, see the url: http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

The following table lists the hardware supported on the Catalyst 4900M Series Switch.

Table 1 Supported Hardware for Catalyst 4900M Series Switch

Product Number (append with "=" for spares)	**Product Description**
WS-C4900M	Catalyst 4900M 8-port base system
WS-X4908-10G-RJ45	8-Port Wire-Speed 10 Gigabit Ethernet (RJ-45) **Note** This linecard is not supported on the Catalyst 4948E Ethernet Switch.
WS-X4920-GB-RJ45 (=)	Catalyst 4900M 20-port 10/100/1000 RJ-45 half card
WS-X4904-10GE (=)	Catalyst 4900M 4 port 10GbE half card with X2 interfaces
WS-X4908-10GE (=)	Catalyst 4900M 8 port 10GbE half card with X2 interfaces
WS-X4908-10G-RJ45	8 port 10 Gigabit linecard with 2 to 1 oversubscription
WS-X4994	Blank PS Cover
WS-X4994=	Blank PS Cover Spare
WS-X4993=	Spare Fan Tray
PWR-C49M-1000AC(=)	Catalyst 4900M AC Power Supply
PWR-C49M-1000AC/2	Catalyst 4900M AC Power Supply Redundant
PWR-C49M-1000DC(=)	Catalyst 4900M DC Power Supply
PWR-C49M-1000DC/2	Catalyst 4900M DC Power Supply Redundant
WS-X4992=	Catalyst 4900M Spare Fan Tray
WS-X4994	Blank PS Cover
WS-X4994=	Blank PS Cover Spare
WS-X4993=	Spare Fan Tray
CVR-X2-SFP=	TwinGig converter module

The following table lists the hardware supported on the Catalyst 4948E Ethernet Switch.

Table 2 Supported Hardware for Catalyst 4948E Ethernet Switch

Product Number (append with "=" for spares)	**Product Description**
WS-C4948E	48x 10/100/1000(RJ45)+4x 10GbE(SFP+), no p/s
WS-C4948E-S	48x 10/100/1000(RJ45)+4x10GbE(SFP+), IP Base IOS, AC p/s

Table 2 Supported Hardware for Catalyst 4948E Ethernet Switch

Product Number (append with "=" for spares)	**Product Description**
WS-C4948E-E	48x 10/100/1000(RJ45)+4x10GbE(SFP+), Ent Ser IOS, AC p/s
WS-C4948E-BDL	Green Bundle 10x WS-C4948E
PWR-C49E-300AC-R=	Catalyst 4948E 300WAC power supply (spare)
PWR-C49E-300AC-R/2	Catalyst 4948E 300WAC redundant power supply
PWR-C49-300DC=	Catalyst 4948E 300WDC power supply (spare)
PWR-C49-300DC/2	Catalyst 4948E 300WDC redundant power supply (spare)
WS-X4993-F(=)	Cisco Catalyst 4948E spare fan tray rear exhaust

The following table lists the hardware supported on the Catalyst 4948E-F Ethernet Switch.

Table 3 Supported Hardware for Catalyst 4948E-F Ethernet Switch

Product Number (append with "=" for spares)	**Product Description**
WS-C4948E-F	48x 10/100/1000(RJ45)+4x 10GbE(SFP+), no p/s
WS-C4948E-F-S	48x 10/100/1000(RJ45)+4x10GbE(SFP+), IP Base IOS, AC p/s
WS-C4948E-F-E	48x 10/100/1000(RJ45)+4x10GbE(SFP+), Ent Ser IOS, AC p/s
WS-C4948E-F- BDL	Green Bundle 10x WS-C4948E
PWR-C49E-300AC-F=	Catalyst 4948E 300WAC power supply (spare)
PWR-C49E-300AC-F/2	Catalyst 4948E 300WAC redundant power supply
WS-X4993-F(=)	Cisco Catalyst 4948E spare fan tray rear exhaust

Supported Features

Note The default image for the Catalyst 4900M series switch is Cisco IOS Release 12.2(53)SG2.

Table 4 lists the Cisco IOS software features for the Catalyst 4948E Ethernet Switch and Catalyst 4900M series switches. 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 4 Cisco IOS Software Feature Set for the Catalyst 4948E Ethernet Switch and Catalyst 4900M Series Switches

Layer 2 Switching Features
Storm control

Table 4 Cisco IOS Software Feature Set for the Catalyst 4948E Ethernet Switch and Catalyst 4900M Series Switches

Storm Control: Per-Port Multicast Suppression
Multicast storm control
IP Source Guard
IP Source Guard for Static Hosts
PVRST+
Layer 2 transparent bridging[1]
Layer 2 MAC[2] learning, aging, and switching by software
Unicast MAC address filtering
VMPS[3] Client
Layer 2 hardware forwarding up to 102 Mpps
Layer 2 Control Policing (Not supported on Supervisor Engine 6-E)
Layer 2 switch ports and VLAN trunks
Spanning-Tree Protocol (IEEE 802.1D) per VLAN
802.1s and 802.1w
Layer 2 traceroute
Unidirectional Ethernet port
Per-VLAN spanning tree (PVST) and PVST+
Spanning-tree root guard
Spanning-tree Loop guard and PortFast BPDU Filtering
NEAT Enhancement: Re-Enabling BPDU Guard Based on User Configuration
Enable NEAT or LAN Base
Support for 9216 byte frames
Port security
Port security on Voice VLAN
Port security MAC Aging
Trunk Port Security
Unicast MAC Filtering
802.1X Multiple Domain Authentication and Multiple Authorization
802.1X with ACL Assignment and Redirect URLs
802.1X with per-user ACL and Filter-ID ACL
RADIUS-Provided Session Timeouts
RADIUS CoA
Multi-authentication and VLAN Assignment
MAC Move and Replace
802.1X with Guest VLANs
802.1X with MAC Authentication Bypass
802.1X with Web-Based Authentication

Table 4 Cisco IOS Software Feature Set for the Catalyst 4948E Ethernet Switch and Catalyst 4900M Series Switches

802.1X with Inaccessible Authentication Bypass
802.1X with User Distribution
802.1X with Unidirectional Controlled Port
802.1X with VLAN User Distribution
802.1X with Authentication Failed VLAN Assignment
802.1X with Voice VLAN Ports
802.1X with VLAN Assignment
802.1X with Fallback Authentication
802.1X with Periodic Reauthentication
802.1X with Multiple Hosts
802.1X Supplicant and Authenticator Switches with Network Edge Access Topology
802.1X with Port Security
Cisco TrustSec SGT Exchange Protocol (SXP) IPv4
Private VLANs
Private VLAN DHCP snooping
Private VLAN trunks
2-way Community Private VLANs
PVLAN over EtherChannel
IEEE 802.1Q-based VLAN encapsulation
Multiple VLAN access port
VLAN Trunking Protocol (VTP) and VTP domains
VTP v3
No. of VLAN support per switch: 2048 (for LAN Base) and 4096 (for IP Base)
Unidirectional link detection (UDLD) and aggressive UDLD
Sub-second UDLD (Fast UDLD)
SNMP V3 support for Bridge-MIB with VLAN indexing
IEEE 802.1ag - D8.1 standard Compliant CFM, Y.1731 multicast LBM / AIS / RDI / LCK, IP SLA for Ethernet
Ethernet OAM Protocol
Supported Protocols
DTP[4]
RIPv1[5] and RIPv2, Static Routing
EIGRP[6]
EIGRP Stub Routing
EIGRP Service Advertisement Framework[7]
OSPF[8]
BGP4[9]

Table 4 Cisco IOS Software Feature Set for the Catalyst 4948E Ethernet Switch and Catalyst 4900M Series Switches

BGP 4Byte ASN (CnH)
BGP route-map Continue
BGP Neighbor Policy
MBGP[10]
MSDP[11]
ICMP[12] Router Discovery Protocol
Static routes
Classless interdomain routing (CIDR)
DVMRP[13]
NTP[14]
NTP for IPv6
NTP for VRF aware
NTP master command
STP - Portfast BPDU Guard
STP- BPDU Filtering
STP - Root Guard
SCP[15]
WCCP Version 2
EtherChannel Features
Cisco EtherChannel technology - 10/100/1000 Mbps, 10 Gbps
Load balancing for routed traffic, based on source and destination IP addresses
Load sharing for bridged traffic based on MAC addresses
IEEE 802.1Q on all EtherChannels
Bundling of up to eight Ethernet ports
Trunk Port Security over EtherChannel
Link State Tracking
Additional Protocols and Features
Secure Copy Protocol (SCP)
Link Layer Discovery Protocol (LLDP)
Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED)
PoEP via LLDP
DSCP/CoS via LLDP
IEEE 802.1ab LLDP enhancements (PoE+Layer 2 COS)
ANSI TIA-1057 LLDP - MED Location Extension
ANSI TIA-1057 LLDP - MED Support
Routed Jumbo Frame support
SPAN CPU port mirroring

Table 4 Cisco IOS Software Feature Set for the Catalyst 4948E Ethernet Switch and Catalyst 4900M Series Switches

SPAN packet-type filtering
SPAN destination in-packets option
SPAN ACL filtering
Enhanced VLAN statistics
Secondary addressing
Bootstrap protocol (BOOTP)
Authentication, authorization, and accounting using TACACS+ and RADIUS protocol
TACACS+ and Radius for IPv6-
Critical Authorization for Voice and Data
Cisco Discovery Protocol (CDP)
CDP 2nd Port Status TLV
Propagation of Location Info over CDP
MAC Address-Table Move Update
Flex Link Bi-directional Fast Convergence
Flex Link VLAN Load-Balancing
Flex Links
Flex Links Interface Preemption
Network Mobility Services Protocol
Sticky port security
Voice VLAN Sticky Port Security
Cisco Group Management Protocol (CGMP) server support
HSRP[16] over Ethernet, EtherChannels - 10/100/1000Mbps, 10 Gbps
GLBP
Resilient Ethernet Protocol-no-edge-neighbor-enhancement
VRRP
IGMP[17] snooping version1, version 2, and version 3 (Full Support)
IGMPv3 Host Stack
IGMP filtering
IGMP Querier
Multicast VRF-lite
VRF-aware IP services
VRF-aware TACACS+
Configurable IGMP Leave Timer
Multicast Source Discovery Protocol (MSDP)
SmartPort macros
Auto SmartPort macros
Port Aggregation Protocol (PagP)

Table 4 Cisco IOS Software Feature Set for the Catalyst 4948E Ethernet Switch and Catalyst 4900M Series Switches

802.3ad Link Aggregation (LACP)
802.3ad Link Aggregation (LACP) Port-Channel Standalone Disable
SSH version 1 and version 2[18]
show interface capabilities command
IfIndex persistence
Enhanced SNMP MIB support
SNMP[19] version 1, version 2, and version 3
SNMP version 3 (with encryption)
DHCP server and relay-agent
DHCP Snooping Statistics and SYSLOG
DHCP client autoconfiguration
DHCP Option 82 data Insertion
DHCP Option 82 Pass Through
DHCP Relay Agent for IPv6
DHCP Option 82 - Configurable Remote ID and Circuit ID
Port flood blocking
Router standard and extended ACLs [20]on all ports with no performance penalty
Downloadable ACL
VLAN ACL
PACL[21]
VACL
RACL
Unicast RPF
Local Proxy ARP
Dynamic ARP Inspection on PVLANs
Dynamic ARP Inspection
Per-VLAN CTI
ARP QoS
MQC
Ingress/Egress Policing
Ingress Rate Limiting
Egress Bandwidth Limiting/port shaping
Per VLAN Policy & Per Port Policer
802.1p Priority
Strict Priority Scheduling
Ingress/Egress Strict Priority Queuing (Expedite)
Shaped Round Robin (SRR)

Table 4 Cisco IOS Software Feature Set for the Catalyst 4948E Ethernet Switch and Catalyst 4900M Series Switches

Egress Shaped Queues
Ingress/egress Shared Queues
DSCP Mapping
DSCP Filtering
AutoQoS - VoIP
PBR[22]
Auto QoS 1.5
Trust Boundary Configuration
Dynamic Buffer Limiting (DBL)
Per-VLAN Control Traffic Intercept
Table Map Based Classification
Interface Index Persistence
UDI - Unique Device Identifier
Per-port QoS[23] rate-limiting and shaping
QoS for IPv6
Per-port Per-VLAN QoS
Energy Wise
Two-Rate Three-Color Policing
Dynamic Multi-Protocol Ternary Content Addressable Memory
SmartPort macros
802.1s standards compliance
Flexible Authentication Sequencing
Multi-Authentication
Open Authentication
Web Authentication
Local Web Authentication (EPM syslog and Common session ID)
PPPoE Intermediate Agent
Identity ACL Policy Enforcement[24]
Identity 4.1 Network Edge Access Topology
IPv6 routing - unicast routing "RIPng"
IPv6 Neighbor Discovery Throttling
IPv6 MLDv1 & v2 SNooping
IPv6 Host support (- IPv6 support: Addressing; IPv6: Option processing, Fragmentation, ICMPv6,
TCP/UDP over IPv6; Applications: Ping/Traceroute/VTY/SSH/TFTP, SNMP for IPv6 objects)
IPv6 ACLs
IPv6 Management Services (CDP over IPv6, SSHv2 over IPv6)
IPv6: MLDv1/v2

Table 4 Cisco IOS Software Feature Set for the Catalyst 4948E Ethernet Switch and Catalyst 4900M Series Switches

IPv6:CEFv6
IPv6:MLD Snooping
IPv6 PACL
IPv6 RA Guard
IPv6 Interface Statistics
Non-stop Forwarding Awareness
Non-stop Forwarding Awareness for EIGRP-stub in IP base for all supervisor engines
BGP MIB
OSPF Fast Convergence[25]
AutoRP
Service-Aware Resource Allocation
TwinGig Converter Module
FAT File System
EEM 3.2[26]
VSS client with PagP+
Ethernet Management Port
Enhanced Object Tracking subfeatures: • HSRP with EOT • VRRP with EOT • GLBP with EOT • IP SLA with EOT • Reliable Backup Static Routing with EOT
ANCP Client
CPU Optimization for Layer 3 Multicast Control Packets
Bidiectional PIM
OSPF and EIGRP Fast Convergence
Inactivity Timer
boot config command
Crashdump enhancement
Unicast MAC filtering
Energy Wise
DHCPv6 Ethernet Remote ID option
DHCPv6 Relay - Persistent Interface ID option
DHCPv6 Relay Agent notification for Prefix Delegation
PIM SSM Mapping
VRF lite NSF support with routing protocols OSPF/EIGRP/BG
Layer 2 Tunneling Protocol

Table 4 Cisco IOS Software Feature Set for the Catalyst 4948E Ethernet Switch and Catalyst 4900M Series Switches

Online Diagnostics
PIM Accept Register - Rogue Multicast Server Protection[27]
Configuration Rollback
IP Multicast Load Splitting (Equal Cost Multipath (ECMP) using S, G and Next-hop)
OSPF for Routed Access
Archiving crashfiles
Cisco Network Assistant (CNA)
Per-VLAN Learning
XML Programmatic Interface
VLAN Mapping (VLAN Translation)[28]
GOLD Online Diagnostics
IPSG for Static Hosts
Layer 2 Control Packet
Duplication Location Reporting Issue
NetFlow-lite (on Catalyst 4948E and Catalyst 4948E-F in IP Base or higher)
IOS Based Device profiling
SXP Syslog enhancement
Medianet 2.0 • Monitoring (includes Performance Monitoring and Mediatrace) • Flow MetaData • Media Services Proxy • Integrated video traffic simulator (hardware assisted IP SLA) IPSLA responder only • AutoQoS Macro
Medianet2.0:NMSP enhancements • Location at switch level • Local timezone change • GPS support for location • Priority settings for MIBs • Name value pair
Energy Wise v 2.5
Easy Virtual Network
ND cache limit per interface
HSRPv2 for IPv6 Global Address Support
Identity 4.2: MAB with configurable user name/ password
BGP Wildcard

Table 4 Cisco IOS Software Feature Set for the Catalyst 4948E Ethernet Switch and Catalyst 4900M Series Switches

LACP Independent mode support
VLAN ID support for Flexible NetFlow
Bidirection Forwarding Detection
BGP 4Byte ASN (CnH)
IGMPv3 Host Stack
Per Intf IGMP State Limit
Per Intf MrouteState Limit
TACACS+ and Radius for IPv6-
NTP for IPv6
NTP for VRF aware
IPv6 OSPFv3 NSF/SSO
IPv6 OSPFv3 Fast Convergence
OSPFv3 Authentication
IPsecv3/IKEv2
OSPFv3 authentication
FIPS 140-2/3 Level 2 Certification
No Service Password Recovery
IEEE 802.1X with User Distribution
EIGRP Service Advertisement Framework
EnergyWise 2.5
Identity 4.1 ACL Policy Enhancements
Identity 4.1 Network Edge Access Topology
IS-IS for IPv4 and IPv6
VRF-aware TACACS+
Netflow-lite (on Catalyst 4948E and Catalyst 4948E-F in IP Base or higher)
IPv4 and IPv6 BFD

1. Hardware-based transparent bridging within a VLAN
2. MAC = Media Access Control
3. VMPS = VLAN Management Policy Server
4. DTP = Dynamic Trunking Protocol
5. RIP = Routing Information Protocol
6. EIGRP = Enhanced Interior Gateway Routing Protocol
7. Refer to the URL:http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/saf_cg.html
8. OSPF = Open Shortest Path First
9. BGP4 = Border Gateway Protocol 4
10. MBGP = Multicast Border Gateway Protocol
11. MSDP = Multicast Source Discovery Protocol
12. ICMP = Internet Control Message Protocol
13. DVMRP = Distance Vector Multicast Routing Protocol
14. NTP = Network Time Protocol

15. SCP = Secure Copy Protocol
16. HSRP = Hot Standby Router Protocol
17. IGMP = Internet Group Management Protocol
18. SSH = Secure Shell Protocol
19. SNMP = Simple Network Management Protocol
20. ACLs = Access Control Lists
21. PACL = Port Access Control List
22. Policy-based Routing
23. QoS = Quality of Service
24. filter-ID and per-user ACL
25. The Catalyst 4500 series switch supports Fast Hellos, ISPF, and LSA Throttling.
26. EEM = Embedded Event Manager: Refer to the URL: http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_3.2.html
27. The route-map keyword is not supported.
28. WS-C4948-10GE does not support VLAN mapping.

Unsupported Features

These features are not supported in Cisco IOS Release 15.0(2)SG for the Cisco Catalyst 4948E Ethernet Switch and the Catalyst 4900M series switch:

- The following ACL types:
  - Standard Xerox Network System (XNS) access list
  - Extended XNS access list
  - DECnet access list
  - Protocol type-code access list
- ADSL and Dial access for IPv6
- AppleTalk EIGRP (use native AppleTalk routing instead)
- Auto RP
- AutoQoS - VoIP
- Bridge groups
- CEF Accounting
- CER for E-911 Support
- CFM CoS
- Cisco-Port-QoS-MIB
- Cisco IOS software IPX ACLs:
  - <1200-1299> IPX summary address access list
- Cisco IOS software-based transparent bridging (also called “fallback bridging”)
- Connectionless (CLNS) routing; including IS-IS routing for CLNS. IS-IS is supported for IP routing only.
- DLSw (data-link switching)
- Global QoS (enable QoS)
- HTTP Software Upgrade

- IGRP (use EIGRP instead)
- **isis network point-to-point** command
- ISSU
- Kerberos support for access control
- LLDP HA
- Lock and key
- MAC Address Notification
- MAC notification MIB support
- NAC L2 IP - Inaccessible authentication bypass
- NAT-PT for IPv6
- NSF with SSO
- Packet Based Storm Control
- Reflexive ACLs
- MPLS and routing IP over an MPLS network
- RPR
- Time Domain Reflectometry on pluggable modules
- UniDirectional Link Routing (UDLR)

Orderable Product Numbers

- S49EES-15101SG(=)—Cisco Catalyst 4948E/E-F IOS Enterprise Services w/o CRYPTO
- S49EESK9-15101SG(=)—Cisco Catalyst 4948E/E-F IOS Enterprise Services SSH
- S49EIPB-15101SG(=)—Cisco Catalyst 4948E/E-F IOS IP Base w/o CRYPTO
- S49EIPBK9-15101SG(=)—Cisco Catalyst 4948E/E-F IOS IP Base SSH
- S49ELB-15101SG(=)—Cisco Catalyst 4948E/E-F IOS LAN Base w/o CRYPTO
- S49ELBK9-15101SG(=)—Cisco Catalyst 4948E/E-F IOS LAN Base SSH
- S49MES-15101SG(=)—Cisco Catalyst 4900M IOS Enterprise Services w/o CRYPTO
- S49MESK9-15101SG(=)—Cisco Catalyst 4900M IOS Enterprise Services SSH
- S49MIPB-15101SG(=)—Cisco Catalyst 4900M IOS IP Base w/o CRYPTO
- S49MIPBK9-15101SG(=)—Cisco Catalyst 4900M IOS IP Base SSH

New and Changed Information

These sections describe the new and changed information for the Catalyst 4948E Ethernet Switch and the Catalyst 4900M series switch running Cisco IOS software:

- New Hardware Features in Release 15.1(1)SG1, page 17
- New Software Features in Release 15.1(1)SG1, page 17
- New Hardware Features in Release 15.1(1)SG, page 17

- New Software Features in Release 15.1(1)SG, page 17

New Hardware Features in Release 15.1(1)SG1

Release 15.1(1)SG1 provides no new hardware on the Catalyst 4500 series switch.

New Software Features in Release 15.1(1)SG1

Release 15.1(1)SG1 provides no new new software on the Catalyst 4500 series switch:

New Hardware Features in Release 15.1(1)SG

Release 15.1(1)SG provides the following new hardware for Catalyst 4900M, Catalyst 4948E Ethernet Switch, and Catalyst 4948E-F Ethernet Switch:

- GLC-EX-SMD—1000BASE-EX SFP transceiver module for SMF, 1310-nm wavelength, extended operating temperature range and DOM support, dual LC/PC connector

New Software Features in Release 15.1(1)SG

Release 15.0(2)SG provides the following Cisco IOS software features for Catalyst 4900M and Catalyst 4948E Ethernet Switch:

- IOS Based Device profiling
- SXP Syslog enhancement
- Medianet 2.0
  - Video Monitoring (includes Passive Monitoring and Mediatrace)
  - MetaData
  - MSI Proxy
  - Integrated video traffic simulator (hardware assisted IP SLA)

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

  For details refer to the URLs:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/v2_5/olh/ccp.pdf

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

- IPv6 OSPFv3 NSF/SSO
- IPv6 OSPFv3 Fast Convergence
- OSPFv3 Authentication
- IPsecv3/IKEv2
- OSPFv3 authentication
- FIPS 140-2/3 Level 2 Certification
- No Service Password Recovery
- Easy Virtual Network (EVN)
- ND cache limit per interface
- HSRPv2 for IPv6 Global Address Support
- Identity 4.2: MAB with configurable user name/ password
- BGP Wildcard
- VLAN ID support for Flexible NetFlow
- Bidirectional Forwarding Detection (BFD) Hardware Offload Support
- BFD - EIGRP Support
- BFD - Static Route Support over IPv4
- BFD IPv6 Encapsulation Support
- BGP Support for BFD
- OSPF Support for BFD over IPv4
- OSPFv3 BFD
- Static Route Support for BFD over IPv6
- BGP 4Byte ASN (CnH)
- BGP graceful restart per neighbor
- BGP Nexthop tracking
- Dynamic PBR API
- Multicast Call Admission Control—Per interface route state limit
- Bandwidth-based Call Admission Control policy for Multicast
- Ability to disallow mcast group ranges
- IPv6 SSM mapping—MLD v1 receivers
- IPv6 BSR—Ability to configure RP mapping
- MSDP MD5 password authentication
- MLD group limits
- IPv6 multicast—Disable group ranges
- IGMP static group range support
- PIM-triggered joins
- Support directly conn. add in autoRP cand. RP
- Enhanced Multicast Multipath
- IGMP-STD-MIB implementation

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

Minimum and Recommended ROMMON Release

Table 5 lists the minimum and recommended ROMMON releases for Catalyst 4900M switch and Catalyst 4948E Ethernet Switch.

Table 5 Minimum and Recommended ROMMON Release for Catalyst 4900M and Catalyst 4948E

	Minimum ROMMON Release
Catalyst 4900M Switch	12.2(40r)XO
Catalyst 4948E Ethernet Switch	12.2(44r)SG8

Note ROMMON Release 12.2(44r)SG5 is the minimum required to run Cisco IOS Release 15.0(2)SG and is recommended for other releases.

Limitations and Restrictions

Following limitations and restrictions apply to the Cisco Catalyst 4948E Ethernet Switch and the Catalyst 4900M series switch:

- Starting with Release IOS XE 3.3.0SG and IOS 15.1(1)SG, the seven RP restriction was removed
- The WS-X4920-GB-RJ45 card performs at wire speed until it operates at 99.6% utilization. Beyond this rate, the card will lose some packets.
- Compact Flash is not supported on a Cisco Catalyst 4900M switch running Cisco IOS Release 12.2(40)XO. Attempting to use Compact Flash may corrupt your data.
- 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.
- 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 45 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.
- You can run only .1q-in-.1q packet pass-through with the Catalyst 4948E Ethernet Switch and Catalyst 4900M series switch.
- For PVST, on Catalyst 4948E Ethernet Switch and Catalyst 4948E series switch VLANs, Cisco IOS Release 12.2(t54)SG supports a maximum of 3000 spanning tree port instances. If you want to use more than this number of instances, you should use MST rather than PVST.
- Because the Catalyst 4948E Ethernet Switch and the Catalyst 4900M series switch supports the FAT filesystem, the following restrictions apply:
  - The **verify** and **squeeze** commands are not supported.
  - The **rename** command is supported in FAT file system.

    For the Catalyst 4948E Ethernet Switch and the Catalyst 4900M series switch, the **rename** command has been added for bootflash and slot0. For all other supervisor engines, the **rename** command is supported for nvram devices only.
  - the **fsck** command is supported for slot0 device. It is not supported in the file systems on supervisor engines other than 6-E.
  - In the FAT file system, the IOS **format bootflash:** command erases user files only. It does not erase system configuration.
  - The FAT file system supports a maximum of 63 characters for file/directory name. The maximum for path length is 127 characters.

  - The FAT file system does not support the following characters in file/directory names:{}#%^ and space characters.
  - The FAT file system honors the Microsoft Windows file attribute of "read-only" and "read-write", but it does not support the Windows file "hidden" attribute.
  - Supervisor Engine 6-E uses the FAT file system for compact flash (slot0). If a compact flash is not formatted in FAT file system (such as compact flash on a supervisor engine other than 6-E), the switch does not recognize it.
- The Fast Ethernet port (10/100) 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.
- 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.
- If a Catalyst 4948E Ethernet Switch or a Catalyst 4900M 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.
- 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.
- 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.

- Class-map match statements using **match ip prec | dscp** match only IPv4 packets whereas matches performed with **match prec | dscp** match both IPv4 and IPv6 packets.
- IPv6 QoS hardware switching is disabled if the policy-map contains IPv6 ACL and match cos in the same class-map with the ipv6 access-list has any mask range between /81 and /127. It results in forwarding packets to software which efficiently disable the QoS.
- 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 behavior 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.
- Upstream ports on the Catalyst 4900M and Catalyst 4948E Ethernet Switch support flow control auto negotiation in 1G mode only, and flow control is forced in 10G mode. If the interface is configured to auto-negotiate the flow control, and the interface is operating in 10G mode, the system forces flow control to ON and does not auto-negotiate.
- 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.
  - The Catalyst 4948E Ethernet Switch and the Catalyst 4900 Ethernet switch support fast UDLD on a maximum of 32 ports.

- 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 4900M 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.
- Although you can configure subsecond PIM query intervals on Catalyst 4500 platforms, such an action represents a compromise between convergence (reaction time) and a number of other factors (number of mroutes, base line of CPU utilization, CPU speed, processing overhead per 1 m-route, etc.). You must account for those factors when configuring subsecond PIM timers. We recommend that you set the PIM query interval to a minimum of 2 seconds. By adjusting the available parameters, you can achieve flawless operation; that is, a top number of multicast routes per given convergence time on a specific setup.
- With Cisco IOS Release XE 3.2.1SG, **memory** configuration is enabled:

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

  This configuration had been removed erroneously in a prior release.
- With Cisco IOS Release 12.2(53)SG3 (and 12.2(54)SG), we changed the default behavior such that your single supervisor, RPR, or fixed configuration switch does not reload automatically. To configure automatic reload, you must enter the **diagnostic fpga soft-error recover aggressive** command. (CSCth16953)
- Energywise WOL is not “waking up” a PC in hibernate or standby mode.

  Workaround: None. CSCtr51014
- The ROMMON version number column in the output of **show module** command is truncated.

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

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

  Workaround: None. CSCty79236
- While configuring an IPv6 access-list, if you specify "hardware statistics" as the first statement in v6 access-list mode (i.e. before issuing any other v6 ACE statement), it will not take effect. Similarly, your "hardware statistics" configuration will be missing from the output of the **show running** command.

  Workaround: During IPv6 access-list configuration, configure at least one IPv6 ACE before the "hardware statistics" statement. CSCuc53234

- 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.

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

http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a315.shtml

Open Caveats in Cisco IOS Release 15.1(1)SG2

This section lists the open caveats in Cisco IOS Release 15.1(1)SG2:

- If a class-map is configured with **exceed-action drop**, re-configuring the same class-map with **exceed-action transmit** causes class-map configurations to conflict for the same class-map.

  Workaround: If you plan to change a class-map action, such as **exceed-action**, you meed to remove the class-map with the **no class c1** command under policy-map submode. Then, apply the new class-map with the updated changes. CSCsk70826)

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

  Workaround: Enter the **show policy-map interface** command. CSCsi71036

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

  Workaround: None. However, if you enter the **show policy-map** *name*, the unconditional marking actions are displayed. CSCsi94144

- IGMP snooping entries are active even after disabling IGMP snooping globally and per VLAN.

  Workarounds: Disable IGMP snooping on all the relevant VLANs before disabling it globally.

- IPv6 entries are active in the CAM; the CPU receives IPv6 packets.

  Workaround: Unconfigure any generic QOS policies from the system. The QoS policies with the **match any** attribute cause IPv6 entries to become active. If the switch is a pure Layer 2 device, remove the generic protocol family attributes and narrow it to the protocol family.

  CSCsq84796

- In Cisco IOS Release 12.2(54)SG, if an etherchannel is a member of a flexlink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (flexlink failure)

  Workaround: None. CSCsq99468

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

  You only see this symptom if you did not allocate a VLAN before you configure the IFM, then at a later time allocate the same VLAN.

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

- 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

- Duplicate serial number error messages are reported on switching One X Convertor with SFP+, SFP+, X2 to another port, the inserted port enters a faulty status.

  This problem impacts X2, OneX converters, and SFP+ on the Supervisor Engine 6-E, and linecards.

  Workaround: Remove and reinsert the One X Convertor with SFP+, SFP+ alone, or X2 after some perceivable delay. CSCsu43461

- 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

- On a Catalyst 4900M switch, 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

- When multiple streams of CRC errors are encountered on WS-C4900M configured with OAM Configuration of monitoring the frame errored seconds, OAM does not always report the value of errored frame seconds correctly.

  To observe this issue, the following CLIs are configured with window size as the period for monitoring the errors and a low threshold equal to the number of CRC errored seconds seen/expected.

```
ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low
```

Workaround: Configure a lower value of low threshold such that the frame errors are seen divided into the expected number of frame errored seconds. CSCsy37181

- 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

- When you configure **switchport block multicast** on a switch running Cisco IOS Release 12.2(53)SG1 and later or 12.2(50)SG6 and later, Layer 2 multicast is not blocked.

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

  Workaround: None. CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for 4948E, C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Workaround: None. CSCte51948

- Fast UDLD in aggressive mode may incorrectly errdisable a link in the following scenarios:
  - Fast UDLD peer switch performs SSO.
  - Fast UDLD peer switch is reloaded.
  - One or more interfaces on a fast UDLD peer switch are shut down (or the port mode changes from switchport to routed, and vice versa).

Note To reduce the likelihood of this event, connect at least two physical interfaces between fast UDLD peer switches. You must configure the interfaces with the same neighbor fast hello interval.

Workarounds:

- Reset the error disabled links with the **udld reset** command.
- Configure error disable recovery with the commands **errdisable recovery cause udld** and **errdisable recovery interval** *value (*between 30 and 86400 sec).
- Manually clear errdisable on the local interface with a **shutdown** then a **no shutdown**.

CSCtc99007

- 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

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

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

This issue does not impact functionality.

Workaround: None.

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

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

  Workaround: None. CSCso93282

- If a port channel is created on a Catalyst 4948E Ethernet Switch 1 Gigabit Ethernet SFP upstream interface and one of the interface links goes down, the average convergence time is roughly 3 sec.

  This behavior is not observed on 10 Gigabit Ethernet SFP+ uplink interfaces.

  Workaround: None. CSCth51469

- 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 a packet sampling monitor is applied on a Layer 3 port, which is also configured for Layer 3 RACL, you might observe multiple merged ACL path signatures stemming from merging the sampling and security ACL features. This behavior results in multiple (twice) copies of flattened ACE programmed in the TCAM, wasting ACL TCAM space.

  This issue only impacts Catalyst 4948E and Catalyst 4948E-F Ethernet Switches. It does not impact functionality.

  Workarounds: Do one of the following:

  – Change the interface to a Layer 2 switch port

  – Do not configure an ACL access-list on the same Layer 3 interface where sampling monitor is enabled. CSCtn79032

- When either the RADIUS-server test feature is enabled or RADIUS-server dead-criteria is configured, and either RADIUS-server deadtime is set to 0 or not configured, the RADIUS-server status is not properly relayed to AAA.

  Workaround: Configure both dead-criteria and deadtime.

  ```
  radius-server dead-criteria
  radius-server deadtime
  ```

  CSCtl06706

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

  Workaround: Shutdown the CE-facing interface. Once all the mask-value entries point to the target CE, unshut the CE-facing interface. CSCtl09941

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

  Workaround: Reduce the number of VLAN mappings. CSCtn56208

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

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

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

  Workaround: Unconfigure and reconfigure the service group. CSCtn88087

- When a sampling monitor is configured on a routed port or on a VLAN (an SVI with just one port as a member) and **bidir multicast** is enabled, a packet sample may be exported even though the original multicast packet was not forwarded by the switch.

  This issue only impacts Catalyst 4948E and Catalyst 4948E-F Ethernet Switches.

  Workaround: None. CSCtk97612

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

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

  CSCto27085

- Global WCCP service configuration fails to enable (WCCP global config 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 config. CSCsc88636.

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

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

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

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

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

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

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

Workaround: None. CSCts20229

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

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

  Workarounds:

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

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

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

  Workaround: None. CSCtx95359

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

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

- When you transfer a startup-config to the switch directly without entering **write mem**, and the startup-config contains the **hw-module uplink shared-backplane** command, the four ports on a Supervisor Engine 6-E are not activated in subsequent reloads. The second port of each supervisor engine remains inactive.

  Workaround: Configure **hw-module uplink shared-backplane** from the console or vty, and enter **write mem**. CSCtx43568

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

  ```
  HARDWARE WATCHDOG
  ```

  This message is not observed during a system bootup.

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

- The Mediatrace Initiator may report the status "Abort due to route changed" when a MAC move happens on a switch configured as the Mediatrace Responder that is also connected to a video traffic generator.

  Workaround: None. CSCtt05864

- With IGMP snooping enabled, multicast traffic received through a tunnel interface is not forwarded out the Outgoing Interface List.

  Workaround: Disable IGMP snooping. CSCuc65538

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

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

- A GLC-GE-100FX pluggable may not operate when used in WS-X4624-SFP-E, WS-X4640-CSFP-E or WS-X4612-SFP-E modules.

Workaround: None CSCui23911

Resolved Caveats in Cisco IOS Release 15.1(1)SG2

This section lits the resolved caveats in Cisco Release 15.1(1)SG2:

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

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

Open Caveats in Cisco IOS Release 15.1(1)SG1

This section lists the open caveats in Cisco IOS Release 15.1(1)SG1:

- If a class-map is configured with **exceed-action drop**, re-configuring the same class-map with **exceed-action transmit** causes class-map configurations to conflict for the same class-map.

  Workaround: If you plan to change a class-map action, such as **exceed-action**, you meed to remove the class-map with the **no class c1** command under policy-map submode. Then, apply the new class-map with the updated changes. CSCsk70826)

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

  Workaround: Enter the **show policy-map interface** command. CSCsi71036

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

  Workaround: None. However, if you enter the **show policy-map** *name*, the unconditional marking actions are displayed. CSCsi94144

- IGMP snooping entries are active even after disabling IGMP snooping globally and per VLAN.

  Workarounds: Disable IGMP snooping on all the relevant VLANs before disabling it globally.

- IPv6 entries are active in the CAM; the CPU receives IPv6 packets.

  Workaround: Unconfigure any generic QOS policies from the system. The QoS policies with the **match any** attribute cause IPv6 entries to become active. If the switch is a pure Layer 2 device, remove the generic protocol family attributes and narrow it to the protocol family.

  CSCsq84796

- In Cisco IOS Release 12.2(54)SG, if an etherchannel is a member of a flexlink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (flexlink failure)

  Workaround: None. CSCsq99468

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

  You only see this symptom if you did not allocate a VLAN before you configure the IFM, then at a later time allocate the same VLAN.

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

- 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

- Duplicate serial number error messages are reported on switching One X Convertor with SFP+, SFP+, X2 to another port, the inserted port enters a faulty status.

  This problem impacts X2, OneX converters, and SFP+ on the Supervisor Engine 6-E, and linecards.

  Workaround: Remove and reinsert the One X Convertor with SFP+, SFP+ alone, or X2 after some perceivable delay. CSCsu43461

- 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

- On a Catalyst 4900M switch, 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

- When multiple streams of CRC errors are encountered on WS-C4900M configured with OAM Configuration of monitoring the frame errored seconds, OAM does not always report the value of errored frame seconds correctly.

  To observe this issue, the following CLIs are configured with window size as the period for monitoring the errors and a low threshold equal to the number of CRC errored seconds seen/expected.

```
ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low
```

  Workaround: Configure a lower value of low threshold such that the frame errors are seen divided into the expected number of frame errored seconds. CSCsy37181

- 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

- When you configure **switchport block multicast** on a switch running Cisco IOS Release 12.2(53)SG1 and later or 12.2(50)SG6 and later, Layer 2 multicast is not blocked.

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

  Workaround: None. CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for 4948E, C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Workaround: None. CSCte51948

- Fast UDLD in aggressive mode may incorrectly errdisable a link in the following scenarios:
  - Fast UDLD peer switch performs SSO.
  - Fast UDLD peer switch is reloaded.
  - One or more interfaces on a fast UDLD peer switch are shut down (or the port mode changes from switchport to routed, and vice versa).

Note To reduce the likelihood of this event, connect at least two physical interfaces between fast UDLD peer switches. You must configure the interfaces with the same neighbor fast hello interval.

  Workarounds:
  - Reset the error disabled links with the **udld reset** command.
  - Configure error disable recovery with the commands **errdisable recovery cause udld** and **errdisable recovery interval** *value (*between 30 and 86400 sec).
  - Manually clear errdisable on the local interface with a **shutdown** then a **no shutdown**.

  CSCtc99007

- 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

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

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

  This issue does not impact functionality.

  Workaround: None.

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

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

  Workaround: None. CSCso93282

- If a port channel is created on a Catalyst 4948E Ethernet Switch 1 Gigabit Ethernet SFP upstream interface and one of the interface links goes down, the average convergence time is roughly 3 sec.

  This behavior is not observed on 10 Gigabit Ethernet SFP+ uplink interfaces.

  Workaround: None. CSCth51469

- 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 a packet sampling monitor is applied on a Layer 3 port, which is also configured for Layer 3 RACL, you might observe multiple merged ACL path signatures stemming from merging the sampling and security ACL features. This behavior results in multiple (twice) copies of flattened ACE programmed in the TCAM, wasting ACL TCAM space.

  This issue only impacts Catalyst 4948E and Catalyst 4948E-F Ethernet Switches. It does not impact functionality.

  Workarounds: Do one of the following:
  - Change the interface to a Layer 2 switch port
  - Do not configure an ACL access-list on the same Layer 3 interface where sampling monitor is enabled. CSCtn79032

- When either the RADIUS-server test feature is enabled or RADIUS-server dead-criteria is configured, and either RADIUS-server deadtime is set to 0 or not configured, the RADIUS-server status is not properly relayed to AAA.

  Workaround: Configure both dead-criteria and deadtime.

  ```
  radius-server dead-criteria
  radius-server deadtime
  ```

  CSCtl06706

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

Workaround: Shutdown the CE-facing interface. Once all the mask-value entries point to the target CE, unshut the CE-facing interface. CSCtl09941

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

  Workaround: Reduce the number of VLAN mappings. CSCtn56208

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

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

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

  Workaround: Unconfigure and reconfigure the service group. CSCtn88087

- When a sampling monitor is configured on a routed port or on a VLAN (an SVI with just one port as a member) and **bidir multicast** is enabled, a packet sample may be exported even though the original multicast packet was not forwarded by the switch.

  This issue only impacts Catalyst 4948E and Catalyst 4948E-F Ethernet Switches.

  Workaround: None. CSCtk97612

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

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

  CSCto27085

- Global WCCP service configuration fails to enable (WCCP global config 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 config. CSCsc88636.

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

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

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

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

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

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

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

  Workaround: None. CSCts20229

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

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

  Workarounds:

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

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

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

  Workaround: None. CSCtx95359

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

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

- When you transfer a startup-config to the switch directly without entering **write mem**, and the startup-config contains the **hw-module uplink shared-backplane** command, the four ports on a Supervisor Engine 6-E are not activated in subsequent reloads. The second port of each supervisor engine remains inactive.

  Workaround: Configure **hw-module uplink shared-backplane** from the console or vty, and enter **write mem**. CSCtx43568

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

  ```
  HARDWARE WATCHDOG
  ```

  This message is not observed during a system bootup.

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

- The Mediatrace Initiator may report the status "Abort due to route changed" when a MAC move happens on a switch configured as the Mediatrace Responder that is also connected to a video traffic generator.

  Workaround: None. CSCtt05864

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

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

- An ISSU upgrade from Cisco IOS 15.0(2)SG5 to 15.1(1)SG1 fails.

  However, you can perform an upgrade from Cisco IOS 15.0(2)SG5 to 15.1(1)SG2 or from Cisco IOS 15.0(2)SG5 to 15.1(2)SG.

  Workarounds:

  – Use RPR for Cisco IOS 15.0(2)SG5 or 15.1(1)SG1 combinations (upgrade or downgrade).

  – Downgrade from Cisco IOS 15.1(1)SG1; using 15.0(2)SG4 or an earlier release.

  – Upgrade from Cisco IOS 15.0(2)SG5; use 15.1(1)SG2 instead.

CSCuc54012

- With IGMP snooping enabled, multicast traffic received through a tunnel interface is not forwarded out the Outgoing Interface List.

  Workaround: Disable IGMP snooping. CSCuc65538

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

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

- A GLC-GE-100FX pluggable may not operate when used in WS-X4624-SFP-E, WS-X4640-CSFP-E or WS-X4612-SFP-E modules.

  Workaround: None CSCui23911

Resolved Caveats in Cisco IOS Release 15.1(1)SG1

This section lists the resolved caveats in Cisco Release 15.1(1)SG1:

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

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

  CSCtz11352

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

  Workaround: None. CSCua12869

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

  Workaround: None. The message is information only. CSCtw93140

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

  – A switchport is configured with both of the following:

    authentication event server dead action authorize...

    authentication event server alive action reinitalize

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

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

  Workaround: None. CSCtx61557

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

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

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

- If either the active or standby supervisor engine is running Cisco IOS 15.1(1)SG, the standby supervisor engine does achieve a standby-cold or standby-hot state; it continues to reload.

Workaround: Downgrade or upgrade the supervisor engine by either temporarily removing the other supervisor engine or relocating the supervisor engine to another chassis. CSCtz44577

- On a switch running Cisco 15.0(2)SG4 or 15.1(1)SG with 4648* or 4748* linecards with PoE, a single port on a linecard fails to link up, usually after flapping its link frequently.

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

- On a switch running Cisco 15.0(2)SG4 or 15.1(1)SG on 4648* or 4748* linecards with PoE, the PoE device will not power up on a single port, but will work on other ports on the same linecard.

  Workarounds:

  - Connect a non-PoE device to the port
  - Enter shut then no shut on the port. CSCua63562

- The Catalyst 4500E series switch with Supervisor Engine 7L-E contains a denial of service (DoS) vulnerability when processing specially crafted packets that can cause a reload of the device.

  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-20120926-ecc

  CSCty88456

- Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp

  CSCty96049

Open Caveats in Cisco IOS Release 15.1(1)SG

This section lists the open caveats in Cisco IOS Release 15.1(1)SG:

- If a class-map is configured with **exceed-action drop**, re-configuring the same class-map with **exceed-action transmit** causes class-map configurations to conflict for the same class-map.

  Workaround: If you plan to change a class-map action, such as **exceed-action**, you meed to remove the class-map with the **no class c1** command under policy-map submode. Then, apply the new class-map with the updated changes. CSCsk70826)

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

  Workaround: Enter the **show policy-map interface** command. CSCsi71036

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

  Workaround: None. However, if you enter the **show policy-map** *name*, the unconditional marking actions are displayed. CSCsi94144

- IGMP snooping entries are active even after disabling IGMP snooping globally and per VLAN.

  Workarounds: Disable IGMP snooping on all the relevant VLANs before disabling it globally.

- IPv6 entries are active in the CAM; the CPU receives IPv6 packets.

  Workaround: Unconfigure any generic QOS policies from the system. The QoS policies with the **match any** attribute cause IPv6 entries to become active. If the switch is a pure Layer 2 device, remove the generic protocol family attributes and narrow it to the protocol family.

  CSCsq84796

- In Cisco IOS Release 12.2(54)SG, if an etherchannel is a member of a flexlink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (flexlink failure)

  Workaround: None. CSCsq99468

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

  You only see this symptom if you did not allocate a VLAN before you configure the IFM, then at a later time allocate the same VLAN.

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

- 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

- Duplicate serial number error messages are reported on switching One X Convertor with SFP+, SFP+, X2 to another port, the inserted port enters a faulty status.

  This problem impacts X2, OneX converters, and SFP+ on the Supervisor Engine 6-E, and linecards.

  Workaround: Remove and reinsert the One X Convertor with SFP+, SFP+ alone, or X2 after some perceivable delay. CSCsu43461

- 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

- On a Catalyst 4900M switch, 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

- When multiple streams of CRC errors are encountered on WS-C4900M configured with OAM Configuration of monitoring the frame errored seconds, OAM does not always report the value of errored frame seconds correctly.

  To observe this issue, the following CLIs are configured with window size as the period for monitoring the errors and a low threshold equal to the number of CRC errored seconds seen/expected.

  ```
  ethernet oam link-monitor frame-seconds window
  ethernet oam link-monitor frame-seconds threshold low
  ```

  Workaround: Configure a lower value of low threshold such that the frame errors are seen divided into the expected number of frame errored seconds. CSCsy37181

- 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

- When you configure **switchport block multicast** on a switch running Cisco IOS Release 12.2(53)SG1 and later or 12.2(50)SG6 and later, Layer 2 multicast is not blocked.

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

  Workaround: None. CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for 4948E, C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Workaround: None. CSCte51948

- Fast UDLD in aggressive mode may incorrectly errdisable a link in the following scenarios:
  - Fast UDLD peer switch performs SSO.
  - Fast UDLD peer switch is reloaded.
  - One or more interfaces on a fast UDLD peer switch are shut down (or the port mode changes from switchport to routed, and vice versa).

Note To reduce the likelihood of this event, connect at least two physical interfaces between fast UDLD peer switches. You must configure the interfaces with the same neighbor fast hello interval.

Workarounds:

- Reset the error disabled links with the **udld reset** command.
- Configure error disable recovery with the commands **errdisable recovery cause udld** and **errdisable recovery interval** *value (*between 30 and 86400 sec).
- Manually clear errdisable on the local interface with a **shutdown** then a **no shutdown**.

CSCtc99007

- 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

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

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

  This issue does not impact functionality.

  Workaround: None.

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

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

  Workaround: None. CSCso93282

- If a port channel is created on a Catalyst 4948E Ethernet Switch 1 Gigabit Ethernet SFP upstream interface and one of the interface links goes down, the average convergence time is roughly 3 sec.

  This behavior is not observed on 10 Gigabit Ethernet SFP+ uplink interfaces.

  Workaround: None. CSCth51469

- 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 a packet sampling monitor is applied on a Layer 3 port, which is also configured for Layer 3 RACL, you might observe multiple merged ACL path signatures stemming from merging the sampling and security ACL features. This behavior results in multiple (twice) copies of flattened ACE programmed in the TCAM, wasting ACL TCAM space.

  This issue only impacts Catalyst 4948E and Catalyst 4948E-F Ethernet Switches. It does not impact functionality.

  Workarounds: Do one of the following:

  - Change the interface to a Layer 2 switch port
  - Do not configure an ACL access-list on the same Layer 3 interface where sampling monitor is enabled. CSCtn79032

- When either the RADIUS-server test feature is enabled or RADIUS-server dead-criteria is configured, and either RADIUS-server deadtime is set to 0 or not configured, the RADIUS-server status is not properly relayed to AAA.

  Workaround: Configure both dead-criteria and deadtime.

  ```
  radius-server dead-criteria
  radius-server deadtime
  ```

  CSCtl06706

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

  Workaround: Shutdown the CE-facing interface. Once all the mask-value entries point to the target CE, unshut the CE-facing interface. CSCtl09941

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

  Workaround: Reduce the number of VLAN mappings. CSCtn56208

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

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

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

  Workaround: Unconfigure and reconfigure the service group. CSCtn88087

- When a sampling monitor is configured on a routed port or on a VLAN (an SVI with just one port as a member) and **bidir multicast** is enabled, a packet sample may be exported even though the original multicast packet was not forwarded by the switch.

  This issue only impacts Catalyst 4948E and Catalyst 4948E-F Ethernet Switches.

  Workaround: None. CSCtk97612

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

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

  CSCto27085

- Global WCCP service configuration fails to enable (WCCP global config 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 config. CSCsc88636.

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

  Workaround: Remove these operators from any dynamic ACLs. CSCts05302

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

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

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

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

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

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

  Workaround: None. CSCts20229

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

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

  Workarounds:

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

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

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

  Workaround: None. CSCtx95359

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

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

- When you transfer a startup-config to the switch directly without entering **write mem**, and the startup-config contains the **hw-module uplink shared-backplane** command, the four ports on a Supervisor Engine 6-E are not activated in subsequent reloads. The second port of each supervisor engine remains inactive.

  Workaround: Configure **hw-module uplink shared-backplane** from the console or vty, and enter **write mem**. CSCtx43568

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

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

  CSCtz11352

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

  ```
  HARDWARE WATCHDOG
  ```

  This message is not observed during a system bootup.

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

- The Mediatrace Initiator may report the status "Abort due to route changed" when a MAC move happens on a switch configured as the Mediatrace Responder that is also connected to a video traffic generator.

  Workaround: None. CSCtt05864

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

  Workaround: None. CSCua12869

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

  Workaround: None. The message is information only. CSCtw93140

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

  – A switchport is configured with both of the following:

  authentication event server dead action authorize...

  authentication event server alive action reinitalize

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

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

  Workaround: None. CSCtx61557

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

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

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

- If either the active or standby supervisor engine is running Cisco IOS 15.1(1)SG, the standby supervisor engine does achieve a standby-cold or standby-hot state; it continues to reload.

  Workaround: Downgrade or upgrade the supervisor engine by either temporarily removing the other supervisor engine or relocating the supervisor engine to another chassis. CSCtz44577

- On a switch running Cisco 15.0(2)SG4 or 15.1(1)SG with 4648* or 4748* linecards with PoE, a single port on a linecard fails to link up, usually after flapping its link frequently.

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

- On a switch running Cisco 15.0(2)SG4 or 15.1(1)SG on 4648* or 4748* linecards with PoE, the PoE device will not power up on a single port, but will work on other ports on the same linecard.

  Workarounds:

  - Connect a non-PoE device to the port
  - Enter shut then no shut on the port. CSCua63562

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

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

- With IGMP snooping enabled, multicast traffic received through a tunnel interface is not forwarded out the Outgoing Interface List.

  Workaround: Disable IGMP snooping. CSCuc65538

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

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

- A GLC-GE-100FX pluggable may not operate when used in WS-X4624-SFP-E, WS-X4640-CSFP-E or WS-X4612-SFP-E modules.

  Workaround: None CSCui23911

Resolved Caveats in Cisco IOS Release 15.1(1)SG

This section lists the resolved caveats in Release 15.1(1)SG:

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

  Workaround: Enter **shut** and **no shut** on the ports. CSCtn88228

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

  Workaround: None. CSCto59368

Troubleshooting

These sections provide troubleshooting guidelines for the Catalyst 4900M series switch running IOS supervisor engines:

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>
```

Note The Catalyst 4948E does not contain a compact flash slot.

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

```
rommon 3> boot tftp://172.16.1.8/tftpboot/cat4500-ipbase-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. An Ethernet cable plugged into the Ethernet port is active only in ROMMON mode.

Troubleshooting Modules

This section contains troubleshooting guidelines for the Catalyst 4900M 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 4900M 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, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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