



Release Notes for the Catalyst 4900M Series Switch, Cisco IOS Release 12.2(46)SG

Current Release
12.2(46)SG—July 2, 2008

Previous Release
12.2(40)X0

These release notes describe the features, modifications, and caveats for Cisco IOS software on the Catalyst 4900M switch.

Cisco Systems announces the Cisco Catalyst 4900M Series, 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 GbE servers or all 10GbE 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.

Support for Cisco IOS Software Release 12.2(46)SG follows the standard Cisco Systems® support policy, available at http://www.cisco.com/en/US/products/products_end-of-life_policy.html

For more information about the Cisco Catalyst 4900M Series, visit: <http://www.cisco.com/go/4900>.



Note

Although their *Release Notes* are unique, the 4 platforms (Catalyst 4500, Catalyst 4900, Catalyst M4900, and Catalyst 4900M) use the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide*. Refer to this location:

http://www.cisco.com/en/US/products/hw/switches/ps4324/tsd_products_support_series_home.html



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

© 2008 Cisco Systems, Inc. All rights reserved.

Contents

This publication consists of these sections:

- [Cisco IOS Software Packaging for the Cisco Catalyst 4900M Switch, page 2](#)
- [System Requirements, page 2](#)
- [Minimum and Recommended ROMMON Release, page 12](#)
- [Limitations and Restrictions, page 12](#)
- [Caveats, page 15](#)
- [Troubleshooting, page 26](#)
- [Related Documentation, page 28](#)
- [Notices, page 30](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 32](#)

Cisco IOS Software Packaging for the Cisco Catalyst 4900M Switch

Catalyst 4900M software features based on Cisco IOS Software 12.2(46)SG will support the IP Base image and the entservices image.

The IP Base image does not support enhanced routing features such as Nonstop Forwarding/Stateful Switchover (NSF/SSO), BGP, Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), Internetwork Packet Exchange (IPX), AppleTalk, Virtual Routing Forwarding (VRF-lite), GLBP, and policy-based routing (PBR). The IP Base image supports Static routes, RIPv1/v2 for IP BASE, and EIGRP-Stub for limited routing on Cisco Catalyst 4900 Series Switches.

The Enterprise Services image supports Cisco Catalyst 4900M Series software features based on Cisco IOS Software 12.2(46)SG, including enhanced routing. BGP capability is included in the Enterprises Services package.

Orderable Product Numbers:

- S45EIPB-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (IP Base Image)
- S45IPBK9-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (IP Base Image with 3DES) (cat4500-ipbasek9-mz)
- S45EES-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image) (cat4500-ipbasek9-mz)
- S45EESK9-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image) (cat4500-ipbasek9-mz)

System Requirements

This section describes the system requirements:

- [Supported Hardware, page 3](#)
- [Supported Features, page 4](#)

- [Unsupported Features, page 9](#)

Supported Hardware

The following tables lists the hardware supported on the Catalyst 4900M series switch.

Table 1 Supported Hardware

Product Number (append with “=” for spares)	Product Description
Small Form-Factor Pluggable Modules (supported only in WS-X4908-10GE(=) half-card)	
GLC-SC-MM	Gigabit Ethernet SFP, LC connector, and SX transceiver small form-factor pluggable module
GLC-LH-SM	Gigabit Ethernet SFP, LC connector, and LX/LH transceiver small form-factor pluggable module
GLC-ZX-SM	1000BASE-ZX small form-factor pluggable module
GLC-T	1000BASE-T small form-factor pluggable module
CWDM-SFP-xxxx	CWDM small form-factor pluggable module (See Table 2 on page 3 for a list of supported wavelengths.)
10 Gigabit Ethernet X2 Pluggable Modules	
X2-10GB-LR	10GBASE-LR X2 transceiver module for SMF, 1310-nm wavelength, SC duplex connector
X2-10GB-ER	10GBASE-ER X2 transceiver module for SMF, 1550-nm wavelength, SC duplex connector
X2-10GB-CX4	10GBASE-CX4 X2 transceiver module for CX4 cable, copper, Infiniband 4X connector
X2-10GB-LX4	10GBASE-LX4 X2 transceiver module for MMF, 1310-nm wavelength, SC duplex connector
X2-10GB-LRM	10GBASE-LRM X2 transceiver module for MMF, 1310-nm wavelength, SC duplex connector
X2-10GB-SR	10GBASE-SR X2 transceiver module for MMF, 850-nm wavelength, SC duplex connector

[Table 2](#) briefly describes the supported wavelengths in the Catalyst 4900M series switches.

Table 2 CWDM SFP Supported Wavelengths

Product Number (append with “=” for spares)	Product Description
CWDM-SFP -1470	Longwave 1470 nm laser single-mode
CWDM- SFP -1490	Longwave 1490 nm laser single-mode
CWDM-SFP -1510	Longwave 1510 nm laser single-mode
CWDM-SFP -1530	Longwave 1530 nm laser single-mode
CWDM-SFP -1550	Longwave 1550 nm laser single-mode

Table 2 CWDM SFP Supported Wavelengths

Product Number (append with “=” for spares)	Product Description
CWDM-SFP -1570	Longwave 1570 nm laser single-mode
CWDM-SFP -1590	Longwave 1590 nm laser single-mode
CWDM-SFP -1610	Longwave 1610 nm laser single-mode

The following tables lists the hardware supported on the Catalyst 4900M series switch.

Table 3 Supported Hardware

Product Number (append with “=” for spares)	Product Description
WS-C4900M	Catalyst 4900M 8-port base system
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
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
CVR-X2-SFP=	TwinGig module

Supported Features

Table 4 lists the Cisco IOS software features for the Catalyst 4900M series switch.

Table 4 Cisco IOS Software Feature Set for the Catalyst 4900M series Switch

Layer 2 Switching Features
Storm control
Storm Control: Per-Port Multicast Suppression
Multicast storm control
IP Source Guard
IP Source Guard for Static Hosts
PVRST+
Layer 2 protocol tunneling
Layer 2 transparent bridging ¹
Layer 2 MAC ² learning, aging, and switching by software
Unicast MAC address filtering

Table 4 Cisco IOS Software Feature Set for the Catalyst 4900M series Switch (continued)

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
Support for 9216 byte frames
Port security
Port security on Voice VLAN
Port security MAC Aging
Trunk Port Security
Unicast MAC Filtering
802.1X with Port Security
Private VLANs
Private VLAN DHCP snooping
IEEE 802.1Q-based VLAN encapsulation
Multiple VLAN access port
VLAN Trunking Protocol (VTP) and VTP domains
Support for 4096 VLANs per switch
Unidirectional link detection (UDLD) and aggressive UDLD
SNMP V3 support for Bridge-MIB with VLAN indexing
Ethernet CFM
Ethernet OAM Protocol
Supported Protocols
DTP ⁴
RIPv1 ⁵ and RIPv2, Static Routing
EIGRP ⁶
EIGRP Stub Routing
OSPF ⁷
BGP4 ⁸
BGP route-map Continue
BGP Neighbor Policy

Table 4 Cisco IOS Software Feature Set for the Catalyst 4900M series Switch (continued)

MBGP ⁹
MSDP ¹⁰
ICMP ¹¹ Router Discovery Protocol
Static routes
Classless interdomain routing (CIDR)
DVMRP ¹²
NTP ¹³
STP - Portfast BPDU Guard
STP- BPDU Filtering
STP - Root Guard
SCP ¹⁴
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
Additional Protocols and Features
Secure Copy Protocol (SCP)
Routed Jumbo Frame support
SPAN CPU port mirroring
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
Cisco Discovery Protocol (CDP)
FlexLink and MAC Address-Table Move Update
Sticky port security
Voice VLAN Sticky Port Security
Cisco Group Management Protocol (CGMP) server support
HSRP ¹⁵ over Ethernet, EtherChannels - 10/100/1000Mbps, 10 Gbps
GLBP
VRRP

Table 4 Cisco IOS Software Feature Set for the Catalyst 4900M series Switch (continued)

IGMP ¹⁶ snooping version 1, version 2, and version 3 (Full Support)
IGMP filtering
IGMP Querier
Configurable IGMP Leave Timer
Multicast Source Discovery Protocol (MSDP)
Smartports I custom macros
Smartports II default macros
Smartports III global macros
Port Aggregation Protocol (PagP)
802.3ad LACP
SSH version 1 and version 2 ¹⁷
show interface capabilities command
IfIndex persistence
Enhanced SNMP MIB support
SNMP ¹⁸ 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 Option 82 - Configurable Remote ID and Circuit ID
Port flood blocking
Router standard and extended ACLs ¹⁹ on all ports with no performance penalty
VLAN Access Control Lists
PACL ²⁰
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

Table 4 Cisco IOS Software Feature Set for the Catalyst 4900M series Switch (continued)

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)
Egress Shaped Queues
Ingress/egress Shared Queues
DSCP Mapping
DSCP Filtering
AutoQoS - VoIP
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 ²¹ rate-limiting and shaping
Per-port Per-VLAN QoS
Two-Rate Three-Color Policing
Dynamic Multi-Protocol Ternary Content Addressable Memory
SmartPort macros
802.1s standards compliance
IPv6 routing - unicast routing "RIPng"
IPv6 Neighbor Discovery Throttingly
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
IPv6:CEFv6
IPv6:MLD Snooping
Non-stop Forwarding Awareness
Non-stop Forwarding Awareness for EIGRP-stub in IP base for all supervisor engines
BGP MIB

Table 4 Cisco IOS Software Feature Set for the Catalyst 4900M series Switch (continued)

OSPF Fast Convergence ²²
AutoRP
Service-Aware Resource Allocation
TwinGig Converter Module
FAT File System
EEM ²³
VSS client with PagP+
Ethernet Management Port
Enhanced Object Tracking
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. OSPF = Open Shortest Path First
8. BGP4 = Border Gateway Protocol 4
9. MBGP = Multicast Border Gateway Protocol
10. MSDP = Multicast Source Discovery Protocol
11. ICMP = Internet Control Message Protocol
12. DVMRP = Distance Vector Multicast Routing Protocol
13. NTP = Network Time Protocol
14. SCP = Secure Copy Protocol
15. HSRP = Hot Standby Router Protocol
16. IGMP = Internet Group Management Protocol
17. SSH = Secure Shell Protocol
18. SNMP = Simple Network Management Protocol
19. ACLs = Access Control Lists
20. PACL = Port Access Control List
21. QoS = Quality of Service
22. The Catalyst 4500 series switch supports Fast Hellos, ISPF, and LSA Throttling.
23. EEM = Embedded Event Manager

Unsupported Features

These features are not supported in Cisco IOS Release 12.2(46)SG for the Catalyst 4900M switch:

- IS-IS
- IS-IS MIB
- Control Plane Policing
- SSM Mapping
- MAC notification MIB support
- RPR
- NSF with SSO

- ISSU
- The following ACL types:
 - Standard Xerox Network System (XNS) access list
 - Extended XNS access list
 - DECnet access list
 - Protocol type-code access list
- ADSL and Dial access for IPv6
- AppleTalk EIGRP (use native AppleTalk routing instead)
- Bridge groups
- Cisco IOS software IPX ACLs:
 - <1200-1299> IPX summary address access list
- Cisco IOS software-based transparent bridging (also called “fallback bridging”)
- Connectionless (CLNS) routing; including IS-IS routing for CLNS. IS-IS is supported for IP routing only.
- DLSw (data-link switching)
- IGRP (use EIGRP instead)
- IP SLA
- **isis network point-to-point** command
- Kerberos support for access control
- Lock and key
- NAT-PT for IPv6
- QoS for IPv6 (QoS for IPv6 traffic)
- Reflexive ACLs
- Routing IPv6 over an MPLS network
- Two-way community VLANs in private VLANs
- WCCP v1 and v2
- PIM Stub in IP Base
- UniDirectional Link Routing (UDLR)
- Policy-Based Routing (PBR)
- NAC L2 IP - Inaccessible authentication bypass
- Packet Based Storm Control
- AutoQoS - VoIP
- Global QoS (enable QoS)
- CER for E-911 Support
- Layer 2 Tunneling Protocol
- Auto RP
- Cisco-Port-QoS-MIB
- Real Time DiagNosis (GOLD-Lite)

- Cisco Network Assistant (CNA)
- TDR
- HTTP Software Upgrade
- MAC Address Notification

New and Changed Information

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

- [New Hardware Features in Release 12.2\(46\)SG, page 11](#)
- [New Software Features in Release 12.2\(46\)SG, page 11](#)

New Hardware Features in Release 12.2(46)SG

Release 12.2(46)SG provides the following new hardware for the Catalyst 4500 series switch:

- None

New Software Features in Release 12.2(46)SG



Note

All features supported in Release 12.2(44)SG on Supervisor Engine 6-E (except for SSO) apply to this chassis.

Release 12.2(46)SG provides the following Cisco IOS software features for the Catalyst 4500 series switch:



Note

The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

- 802.1X Catchup (Refer to the “Configuring 802.1X” chapter)
 - 802.1X Guest VLAN
 - 802.1X Critical Authentication
 - Wake on LAN
 - Radius Accounting
 - Radius Supplied Timeout
- ARP QoS (Refer to the “Configuring QoS” chapter)
- Per-VLAN CTI (Refer to the “Configuring QoS” chapter)
- Flash support for Layer 3 features
- FlexLink and FlexLink+ with MAC Address-Table Move Update (Refer to the “Configuring FlexLink” chapter)

- Ethernet Management Port (Refer to the “Configuring Interfaces” chapter)
- LLDP-MED: location TLV and MIB (Refer to the “Configuring LLDP and LLDP-MED” chapter)
- Enhanced Object Tracking (EOT) ((Refer to the Cisco IOS Release 12.2 documentation)
- RSPAN (Refer to the “Configuring SPAN and RSPAN” chapter)
- CFM 802.3ag (Refer to the “Configuring Ethernet CFM and OAM” chapter)
- E-OAM 802.3ah (Refer to the “Configuring Ethernet CFM and OAM” chapter)
- Ethernet Management Port (Refer to the “Configuring Interfaces” chapter)
- Embedded management (Refer to the Cisco IOS Release 12.4 documentation)
- MAC notify MIB (Refer to the Cisco IOS Release 12.4 documentation)
- BGP (Refer to the Cisco IOS Release 12.4 documentation)
- 802.1X Dynamic VLAN Assignment (Refer to the “Configuring 802.1X” chapter)
- 802.1X MAC Authentication Bypass (Refer to the “Configuring 802.1X” chapter)
- 802.1X with VVID/PVID (Refer to the “Configuring 802.1X” chapter)
- Eight configurable queues per port (Refer to the “Configuring QoS” chapter)
- VSS client with PagP+

Refer to the documentation on the Catalyst 6500 Virtual Switching System at the URL:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod_white_paper0900aecd806ee2ed.html

After configuring VSS dual-active on a Catalyst 6500 switches, the Catalyst 4500 series switch can detect VSS dual-active with PagP+ support.

- IP SLA (Refer to the Cisco IOS Release 12.2 documentation)
- 802.1ab LLDP and 802.1ab LLDP-MED (Refer to the “Configuring LLDP and LLDP-MED” chapter)
- X2 Link Debounce Timer (Refer to the “Configuring Interfaces” chapter)
- Resilient Ethernet Protocol (REP) (Refer to the “Configuring REP” chapter)

Minimum and Recommended ROMMON Release

Table 5 Minimum and Recommended ROMMON Release for Catalyst 4900M

Minimum ROMMON Release	Recommended ROMMON Release
12.2(40r)XO	12.2(44r)SG1

Limitations and Restrictions

- 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 26](#) 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 Catalyst 4900M switch.
- For PVST and Catalyst 4900M switch VLANs, Cisco IOS Release 12.2(40)XO and higher support 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 4900M 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 4900M 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 16,000 IGMP snooping group entries.
- For all software releases, the CLI contains some commands that are not supported. (CSCdw44274)
- Use the **no ip unreachable** 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 4900M 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.

- IPv6 ACL is not supported on a Catalyst 4900M port. IPv6 packets cannot be filtered on switchports using any of the known methods (PACL, VACL, or MACLS).
- Class-map match statements using **match ip prec | dscp** match only IPv4 packets whereas matches performed with **match prec | dscp** match both IPv4 and IPv6 packets.
- IPv6 QoS hardware switching is disabled if the policy-map contains IPv6 ACL and match cos in the same class-map with the ipv6 access-list has any mask 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.

Caveats

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

**Note**

All caveats in Release 12.2 also apply to the corresponding 12.4 E releases. Refer to the *Caveats for Cisco IOS Release 12.2* publication at the following URL:
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124relnt/124cavs/124mcavs.htm>

**Note**

For the latest information on PSIRTS, refer to the Security Advisories on CCO at the following URL:
http://www.cisco.com/en/US/products/products_security_advisories_listing.html

Open Caveats in Cisco IOS Release 12.2(46)SG

This section lists the open caveats in Cisco IOS Release 12.2(46)SG:

- Software qos does not match a .1Q packet properly for applying the desired qos actions.

Workarounds: None.

The support to handle .1Q packets for software QoS lookup unavailable in the Cisco IOS Release 12.2(40)SG release. (CSCsk66449)

- When policer or shape or shape values are specified in terms of percentage of link bandwidth on a policy and the interface on which it is attached is forced to a specific speed with the **speed 10/100/1000** command, the applied policer or shape or shape value might correspond to the new forced speed.

Service policy has to be configured with percentage police or shape or share values and the link speed is forced to a specific values. For example

```
Policy-map p1
  class-map c1
    police rate percent 10
```

Workaround: Either use the **speed auto 10/100/1000** command or the absolute policer, shape or shape values rather than percentage values. For example,

```
Policy-map p1
  class-map c1
    police rate 10 mbps
```

(CSCsk56877)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service-policy.

When an output service-policy is attached to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued to the queue are subjected to the DBL algorithm. If one or more flows are classified as *belligerent* (flows do not back-off in response to drops because of congestion in the queue), those flows continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is non-default (queuing actions are not configured in the class-default class of the policy-map), detach and re-attach the service-policy.

If this happens on the default queue, modifying and resetting some queuing parameters like bandwidth/shape fixes the issue. (CSCsk62457)

- When a Catalyst 4900M switch encounters either a fan tray failure or a supervisor critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to determine the cause of the power-down.

- If the log has *LogGalInsufficientFansDetected* messages, the cause was a fan-tray failure.
- If the log has *LogRkiosModuleShutdownTemp* messages, the cause was that the supervisor critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4900M switch will support a maximum of 32 MTU values system wide. On a Catalyst 4900M running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. Furthermore, MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

Workaround: Reinsert the X2. (CSCsk43618)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you will observe CRC errors after a reload or power cycle when you insert the card or the X2.

Workaround: Reinsert the X2. (CSCsk43618)

- Control plane policing applied to DHCP traffic as identified by the system class-maps system-cpp-dhcp-cs, system-cpp-dhcp-sc, and system-cpp-dhcp-ss may not be effective.

Workaround: None. CSCsk67395)

- When the CPU transmits .1X packet on an interface that has an egress qos policy attached, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original COS value for a .1X packet cannot be matched by software QoS (as per CSCsk66449). The packet is transmitted with whatever COS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured through CSCsk66449, which indicates that the software QoS cannot match against a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, there is no command to check the current operating state.

Workaround: None. You cannot explicitly check the trusted boundary state. However, you can indirectly determine this state:

The trusted boundary feature ensures whether the packet's COS/DSCP value will be trusted or not. When the interface is not in a trusted state, the COS/DSCP fields are forced to zero on a received packet.

A QoS policy exists on that interface that uses that COS/DSCP value for classification. Therefore, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state. (CSCsh72408)

- 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 need to remove the class-map with the **no class c1** command under policy-map submenu. 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)

- You observe a .05% loss on WS-X4908-10GE when sending traffic at 99% of the port capacity.

Workaround: None. (CSCsl39767)

- 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 MLD entries are active even if an IPv6 MLD related configuration does not exist.

Workaround: Unconfigure all generic QOS policies from the system. (CSCsq84853)

- 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)

- Initially, REP configured with VLAN Load Balancing (VLB) works correctly. When you issue a force-switchover on the switch, that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter shut, then no-shut on any REP port (of the same segment in which VLB is configured) in the topology. (CSCso75342)

- In Cisco IOS Release 12.2(46)SG, if flexlink is applied to a pair of etherchannels, then flexlink config may not be applied after a reboot, if the backup EtherChannel is defined after the flexlink configuration.

Workaround: Define the backup etherchannel before applying flexlink command. (CSCsq13477)

- In Cisco IOS Release 12.2(46)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)

- Performing a default interface operation on an interface with auto-QoS enabled results in an error message and the loss of the auto-QoS configuration. For example, the following sequence of operation results in a loss of the configuration:

```
config-if# auto qos voip cisco-phone
config# default interface interface-name
```

Workaround: Replace the **default interface** command with the following:

```
config# interface interface-number
config-if# switchport
```

(CSCsq47116)

- The IPv6 ICMP neighbor state changes from **REACH** to **STALE** after 15 secs of inactivity on the link.

Workaround: Ping the global and link local addresses of the neighbor to ascertain and reinstate reachability. (CSCsq77181)

- IPv6 EIGRP routes are not learned through the port channel.

Workaround: Unconfigure the port channel and the associated physical port, and reconfigure them.

(CSCsq74229)

- 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.

- With CFM, if the VLAN associated with the service instance or MEP is allocated after the Inward Facing MEP (IFM) is configured on an interface whose status is **down**, the IFM CC status remains **inactive** in the output of the **show ethernet CFM maintenance local** command. Also, the CFM remote neighbor is not seen.

This behavior is only seen when VLAN is allocated after the IFM is configured.

Workaround: Unconfigure with the **no ethernet cfm mep level mpid vlan** command, then reconfigure the IFM with the **ethernet cfm mep level mpid vlan** command on the port after the VLAN is allocated. Verify that the C-Status of the IFM is Active with the **show ethernet cfm maintenance-points local** command. (CSCsm85460)

- Occasionally, if a PC continues to send traffic behind an 802.1X capable phone that is plugged into a port configured with MDA (Multi-Domain Authentication), MAB (MAC Authentication Bypass) and port security, a 802.1X security violation is triggered if the port observes traffic from the PC before the phone is fully authorized on the port.

Workaround: Authenticate the phone before plugging a PC behind the phone. (CSCsq92724)

- Ordinarily, the output of a CFM Traceroute from a MEP normally lists down the next hop name(device/host name) for each hop till the other MEP. When CFM over EtherChannel exists between the two MEPs, CFM Traceroute issued from a MEP does not show the next hop name.

Workaround: None. (CSCso50659)

- 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)

- After CFM is disabled globally and then a switch is reloaded with the CFM configuration in place, and after reload when cfm is enabled globally, the cfm meps are being inactive, which results in loss of cfm neighbors.

Workarounds: Do one of the following:

- Reapply the cfm configuration; at a minimum, remove and re-add the MEPs configured on all the interfaces of the switch.
- Deallocate cfm service VLANs and reallocate them.

(CSCsq90598)

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

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

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

Resolved Caveats in Cisco IOS Release 12.2(46)SG

This section lists the resolved caveats in Release 12.2(46)SG:

- When a service-policy is removed from a physical port that is member of an ether channel, a LACP or PAGP protocol-based ether channel goes down. The port-channel members get bundled back in but remain in *suspended* state due to failure to exchange the protocol packets with the other end.

Workarounds: Before removing the service policy from a ether channel member, remove it from the channel. Then, return it to the channel. (CSCsk70568)

- When using *bandwidth percentage* actions in a queuing policy-map, the actual bandwidth share differs from that of the configured policy-map.

In a queuing QoS policy, there can be zero or more queuing classes that have an explicit, user specified, bandwidth share specified. There can be zero or more queuing classes that do not have such user specified bandwidth share. The system takes the unallocated bandwidth share and allocates it equally among the latter set of classes.

When using percentage-based bandwidth allocation, if the share comes to less than 1%, the queues corresponding to those classes do not get updated in hardware with the new bandwidth share. These queues get more than the expected share of bandwidth.

Workarounds: Ensure that the unallocated bandwidth percentage is at least equal to the number of queues that do not have the explicit **bandwidth percentage** command. This should include the default as well as priority queues. (CSCsk77757)

- Not all combinations of features can be simultaneously supported by the hardware. When such a feature combination is configured, packets will be processed in software and a log message indicating this will be generated:

```
%C4K_HWACLMAN-4-ACLHWLABELERR: Path (in :50, 1006) label allocation failure:
SignatureInconsistent - packets will be handled in software, QoS is disabled.
```

One feature combination that can trigger this problem is the attempt to combine a QoS policy that matches on cos bits with IPv6 ACL configuration that matches on IPv6 source addresses that partially mask in the lower 48 bits of the address. (IPv6 subnets in the /81 to /127 range will also trigger this behavior if IPv6 multicast routing is enabled.)

Workaround: Do not configure feature combinations that conflict. Currently the above conflict between QoS policies matching on COS bits and IPv6 configuration with partial masking of the lower 48 bits of the source address is the only known conflicting feature combination. If matching on COS bits is required by the QoS policy, architect the IPv6 network using /80 subnets or larger. (CSCsk79791)

- When a service policy on a port-channel member port is modified, traffic may be dropped for some of the classes.

Workaround: Do the following:

- Un-configure the interface(s) on which this policy-map is attached from the portchannel.
- Modify the policy-map.
- Configure the interface(s) in the portchannel.

(CSCsk77119)

- When two switches are connected back-to-back via two or more links and when a packet is locally-originated, the source IP address may not correspond to the IP address of the outgoing interface. A switch receiving such a packet with unicast RPF feature enabled might drop the incoming packet.

Workaround: None. (CSCsh99124)

- In policy map, if a queuing class with the **bandwidth remaining percent** <> command sits before a priority queuing class configuration, the **bandwidth remaining percent** <> command action is applied on reload.

Workaround: Re-apply the policy-map. (CSCsk75793)

- A hierarchical policy-map can end up having queuing actions at both the parent and child policy-map level. This can happen when the parent class-map already has queuing actions and the child policy-map is modified to have queuing actions.

If such a policy-map is attached to an interface, there will be more than the expected number of queues that will be created.

Workaround: If a hierarchical policy-map is incorrectly configured to have queuing actions at two levels, change either the parent or child policy-map to not have any queuing actions. (CSCsk82028)

- A port can be either a member of a portchannel or have auto-QoS applied to it, but not both. The two are mutually exclusive features.

Currently, if it is applied to a port that is already a member of a portchannel, the application is rejected with an error message. However, the reverse is not true. If auto-QoS is applied first and then the port joins a portchannel, the command is accepted.

The following example using port g2/1 shows the type of usage that should be avoided:

```
conf t
int g2/1
auto qos voice trust
channel-group 10 mode auto
```

This example applies auto-QoS on a port (g2/1) and subsequently makes the port a member of portchannel (10).

Workaround: Do not make a port with auto-QoS enabled a member of a portchannel. (CSCsi95018)

- Policing actions are not applied if they appear at the child level of a two-level hierarchical policy-map.

The switch supports two-level hierarchical policy-maps. Policing actions can be present at only one of the two levels (parent or child). If they are present at the child level, they are not applied.

Workaround: None. (CSCsl06731)

- If *exceed burst* is not explicitly configured for a dual rate policer, the **show policy-map** command displays “0” as the burst value.

Workaround: Enter the **show policy-map interface** command. (CSCsj44237)

- When a queuing policy is attached to a trunk port configured with a per-port per-VLAN QoS policy, the port-level queuing policy is processed as part of a per-VLAN policy and is rejected on bootup. Queuing policy is supported on a physical interface in the output direction only.

Workaround: After bootup, reattach a queuing policy on a physical interface. (CSCsk87548)

- When you delete a port-channel with a per-port per-VLAN QoS policy, the switch crashes.

Workaround: Before deleting the port-channel, do the following:

1. Remove any per-port per-VLAN QoS policies, if any.
2. Remove the VLAN configuration on the port-channel with the **no vlan-range** command. (CSCsk91916)

- The cbQosPoliceCfgTable mib object is *not* populated by the **police bps byte** command.

Workaround: None. (CSCsk45940)

- On rare occasions, a Catalyst 4900M switch may undergo restart if ARP requests are sent to all ports on the switch and “debug ip arp” is enabled.
Workaround: None. (CSCs126706)
- Storm control may not work as expected on TenGig ports 1/1 and 1/3.
Workaround: None. (CSCs137599)

Open Caveats in Cisco IOS Release 12.2(40)XO

This section lists the open caveats in Cisco IOS Release 12.2(40)XO:

- Software qos does not match a .1Q packet properly for applying the desired qos actions.
Workarounds: None.
The support to handle .1Q packets for software QoS lookup unavailable in the Cisco IOS Release 12.2(40)SG release. (CSCsk66449)
- When a service-policy is removed from a physical port that is member of an ether channel, a LACP or PAGP protocol-based ether channel goes down. The port-channel members get bundled back in but remain in *suspended* state due to failure to exchange the protocol packets with the other end.
Workarounds: Before removing the service policy from a ether channel member, remove it from the channel. Then, return it to the channel. (CSCsk70568)
- When using *bandwidth percentage* actions in a queuing policy-map, the actual bandwidth share differs from that of the configured policy-map.
In a queuing QoS policy, there can be zero or more queuing classes that have an explicit, user specified, bandwidth share specified. There can be zero or more queuing classes that do not have such user specified bandwidth share. The system takes the unallocated bandwidth share and allocates it equally among the latter set of classes.
When using percentage-based bandwidth allocation, if the share comes to less than 1%, the queues corresponding to those classes do not get updated in hardware with the new bandwidth share. These queues get more than the expected share of bandwidth.
Workarounds: Ensure that the unallocated bandwidth percentage is at least equal to the number of queues that do not have the explicit **bandwidth percentage** command. This should include the default as well as priority queues. (CSCsk77757)
- Not all combinations of features can be simultaneously supported by the hardware. When such a feature combination is configured, packets will be processed in software and a log message indicating this will be generated:

```
%C4K_HWACLMAN-4-ACLHWLABELERR: Path (in :50, 1006) label allocation failure:
SignatureInconsistent - packets will be handled in software, QoS is disabled.
```


One feature combination that can trigger this problem is the attempt to combine a QoS policy that matches on cos bits with IPv6 ACL configuration that matches on IPv6 source addresses that partially mask in the lower 48 bits of the address. (IPv6 subnets in the /81 to /127 range will also trigger this behavior if IPv6 multicast routing is enabled.)
Workaround: Do not configure feature combinations that conflict. Currently the above conflict between QoS policies matching on COS bits and IPv6 configuration with partial masking of the lower 48 bits of the source address is the only known conflicting feature combination. If matching on COS bits is required by the QoS policy, architect the IPv6 network using /80 subnets or larger. (CSCsk79791)

- When policer or shape or shape values are specified in terms of percentage of link bandwidth on a policy and the interface on which it is attached is forced to a specific speed with the **speed 10/100/1000** command, the applied policer or shape or shape value might correspond to the new forced speed.

Service policy has to be configured with percentage police or shape or share values and the link speed is forced to a specific values. For example

```
Policy-map p1
  class-map c1
    police rate percent 10
```

Workaround: Either use the **speed auto 10/100/1000** command or the absolute policer, shape or shape values rather than percentage values. For example,

```
Policy-map p1
  class-map c1
    police rate 10 mbps
```

(CSCsk56877)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service-policy.

When an output service-policy is attached to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued to the queue are subjected to the DBL algorithm. If one or more flows are classified as *belligerent* (flows do not back-off in response to drops because of congestion in the queue), those flows continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is non-default (queuing actions are not configured in the class-default class of the policy-map), detach and re-attach the service-policy.

If this happens on the default queue, modifying and resetting some queuing parameters like bandwidth/shape fixes the issue. (CSCsk62457)

- When an Catalyst 4900M switch encounters either a fan tray failure or a supervisor critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to determine the cause of the power-down.

- If the log has *LogGallInsufficientFansDetected* messages, the cause was a fan-tray failure.
- If the log has *LogRkiosModuleShutdownTemp* messages, the cause was that the supervisor critical temperature exceeded the failure threshold.

(CSCsk48632)

- When a service policy on a port-channel member port is modified, traffic may be dropped for some of the classes.

Workaround: Do the following:

1. Un-configure the interface(s) on which this policy-map is attached from the portchannel.
2. Modify the policy-map.
3. Configure the interface(s) in the portchannel.

(CSCsk77119)

- When two switches are connected back-to-back via two or more links and when a packet is locally-originated, the source IP address may not correspond to the IP address of the outgoing interface. A switch receiving such a packet with unicast RPF feature enabled might drop the incoming packet.

Workaround: None. (CSCsh99124)

- A Catalyst 4900M switch will support a maximum of 32 MTU values system wide.

On a Catalyst 4900M running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. Furthermore, MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

Workaround: Reinsert the X2. (CSCsk43618)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you will observe CRC errors after a reload or power cycle when you insert the card or the X2.

Workaround: Reinsert the X2. (CSCsk43618)

- Control plane policing applied to DHCP traffic as identified by the system class-maps system-cpp-dhcp-cs, system-cpp-dhcp-sc, and system-cpp-dhcp-ss may not be effective.

Workaround: None. (CSCsk67395)

- In policy map, if a queuing class with the **bandwidth remaining percent** <> command sits before a priority queuing class configuration, the **bandwidth remaining percent** <> command action is applied on reload.

Workaround: Re-apply the policy-map. (CSCsk75793)

- A hierarchical policy-map can end up having queuing actions at both the parent and child policy-map level. This can happen when the parent class-map already has queuing actions and the child policy-map is modified to have queuing actions.

If such a policy-map is attached to an interface, there will be more than the expected number of queues that will be created.

Workaround: If a hierarchical policy-map is incorrectly configured to have queuing actions at two levels, change either the parent or child policy-map to not have any queuing actions. (CSCsk82028)

- When the CPU transmits .1X packet on an interface that has an egress qos policy attached, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original COS value for a .1X packet cannot be matched by software QoS (as per CSCsk66449). The packet is transmitted with whatever COS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured through CSCsk66449, which indicates that the software QoS cannot match against a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, there is no command to check the current operating state.

Workaround: None. You cannot explicitly check the trusted boundary state. However, you can indirectly determine this state:

The trusted boundary feature ensures whether the packet's COS/DSCP value will be trusted or not. When the interface is not in a trusted state, the COS/DSCP fields are forced to zero on a received packet.

A QoS policy exists on that interface that uses that COS/DSCP value for classification. Therefore, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state. (CSCsh72408)

- A port can be either a member of a portchannel or have auto-QoS applied to it, but not both. The two are mutually exclusive features.

Currently, if is applied to a port that is already a member of a portchannel, the application is rejected with an error message. However, the reverse is not true. If auto-QoS is applied first and then the port joins a portchannel, the command is accepted.

The following example using port g2/1 shows the type of usage that should be avoided:

```
conf t
int g2/1
auto qos voice trust
channel-group 10 mode auto
```

This example applies auto-QoS on a port (g2/1) and subsequently makes the port a member of portchannel (10).

Workaround: Do not make a port with auto-QoS enabled a member of a portchannel. (CSCsi95018)

- 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 need to remove the class-map with the **no class c1** command under policy-map submenu. Then, apply the new class-map with the updated changes.

CSCsk70826)

- Policing actions are not applied if they appear at the child level of a two-level hierarchical policy-map.

The switch supports two-level hierarchical policy-maps. Policing actions can be present at only one of the two levels (parent or child). If they are present at the child level, they are not applied.

Workaround: None. (CSCsI06731)

- Applying a policy to a VLAN that has been allocated to a routed port causes the internal VLAN to be policed.

Workaround: Avoid creating a VLAN that has been allocated internally to a routed port. (CSCsh60244)

- If *exceed burst* is not explicitly configured for a dual rate policer, the **show policy-map** command displays “0” as the burst value.

Workaround: Enter the **show policy-map interface** command. (CSCsj44237)

- 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 a queuing policy is attached to a trunk port configured with a per-port per-VLAN QoS policy, the port-level queuing policy is processed as part of a per-VLAN policy and is rejected on bootup.

Queuing policy is supported on a physical interface in the output direction only.

Workaround: After bootup, reattach a queuing policy on a physical interface. (CSCsk87548)

- When you delete a port-channel with a per-port per-VLAN QoS policy, the switch crashes.

Workaround: Before deleting the port-channel, do the following:

1. Remove any per-port per-VLAN QoS policies, if any.
 2. Remove the VLAN configuration on the port-channel with the **no vlan-range** command. (CSCsk91916)
- The cbQosPoliceCfgTable mib object is *not* populated by the **police bps byte** command.
Workaround: None. (CSCsk45940)
 - 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)
 - You observe a .05% loss on WS-X4908-10GE when sending traffic at 99% of the port capacity.
Workaround: None. (CSCsI39767)
 - On rare occasions, a Catalyst 4900M switch may undergo restart if ARP requests are sent to all ports on the switch and “debug ip arp” is enabled.
Workaround: None. (CSCsI26706)
 - Storm control may not work as expected on Tengig ports 1/1 and 1/3.
Workaround: None. (CSCsI37599)

Resolved Caveats in Cisco IOS Release 12.2(40)XO

This section lists the resolved caveats in Release 12.2(40)XO:

- None

Troubleshooting

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

- [Netbooting from the ROMMON, page 26](#)
- [Troubleshooting at the System Level, page 27](#)
- [Troubleshooting Modules, page 27](#)
- [Troubleshooting MIBs, page 28](#)

Netbooting from the ROMMON

Netbooting using a boot loader image is not supported. Instead, use one of the following options to boot an image:

1. Boot from a CompactFlash card by entering the following command:
`rommon 1> boot slot0:<bootable_image>`
2. Use ROMMON TFTP boot.

The ROMMON TFTP boot is very similar to the BOOTLDR TFTP boot, except that:

- the BOOTLDR variable should *not* be set
- the TFTP server must be accessible from the Ethernet management port on the supervisor engine.

To boot from ROMMON, perform the following tasks while in ROMMON mode:

- a. Ensure that the Ethernet management port is physically connected to the network.
- b. Verify that bootloader environment is not set by entering the **unset bootldr** command.
- c. Set IP address of the Ethernet management port on the supervisor engine by entering the following command: **set interface fa1 ip_address <ip_mask**

For example, to set the supervisor engine Ethernet port with an IP address 172.16.1.5 and IP mask 255.255.255.0, enter the following command:

```
rommon 2> set interface fa1 172.16.1.5 255.255.255.0
```

- d. Set default gateway for the Ethernet management port on the supervisor engine by entering the following command: **set ip route default gateway_ip_address**. The default gateway should be directly connected to the supervisor engine Ethernet management port subnet.
- e. Ping the TFTP server to ensure that there is connectivity to the server from the Ethernet management port on the supervisor engine by entering the following command: **ping <tftp_server_ip_address>**.
- f. Once the ping is successful, boot the image from the TFTP server by entering the following command: **boot tftp://tftp_server_ip_address/<image_path_and_file_name**

For example, to boot the image name **cat4500-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

These sections describe the documentation available for the Cisco IOS software for the Catalyst 4900M series switch. These publications consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other publications. Documentation is available electronically or in printed form.

Use these release notes with the publications listed in the following sections:

- [Release-Specific Publications, page 28](#)
- [Platform-Specific Publications, page 28](#)
- [Cisco IOS Software Documentation Set, page 29](#)

Release-Specific Publications

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*
http://www.cisco.com/en/US/products/ps6350/prod_release_notes_list.html



Note

If you have an account on Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, go to Cisco.com and click **Login**. Then go to **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go to <http://www.cisco.com/support/bugtools>.

Platform-Specific Publications

The following publications are available for the Catalyst 4900M series switch running the Cisco IOS software. at the following URL:

- http://www.cisco.com/en/US/products/hw/switches/ps4324/tsd_products_support_series_home.html
- *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
 - *Catalyst 4500 Series Switch Cisco IOS Command Reference*;
http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_command_reference_list.html
 - *Catalyst 4500 Series Switch Cisco IOS System Message Guide*;
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_syst

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting publications.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. You can use each configuration guide in conjunction with its corresponding command reference.

Release 12.2 Documentation Set

The following table describes the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and orderable in printed form.

On Cisco.com at

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/tsd_products_support_series_home.html

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> • <i>Cisco IOS Configuration Fundamentals Command Reference</i> 	Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP and IP Routing Configuration Guide</i> • <i>Cisco IOS IP and IP Routing Command Reference</i> 	IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS Multiservice Applications Configuration Guide</i> • <i>Cisco IOS Multiservice Applications Command Reference</i> 	Multiservice Applications Overview Voice Video Broadband
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping signaling Link Efficiency Mechanisms Quality of Service Solutions

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Other Security Features
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding NetFlow Switching MPLS Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> • <i>New Features in 12.2-Based Limited Lifetime Releases</i> • <i>New Features in Release 12.2 T</i> • Release Notes (release note and caveat documentation for 12.2-based releases and various platforms) • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Dial Services Quick Configuration Guide</i> 	

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 (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

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

This package is an SSL implementation written by Eric Young (ey@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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCDE, CCENT, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0803R)

Release Notes for the Catalyst 4900 Series Switch, Cisco IOS Release 12.2(40)XO
Copyright © 2008, Cisco Systems, Inc. All rights reserved.

