Release Notes for the Cisco Catalyst 4948E-F Ethernet Switch on Release 12.2(54)WO

Current Release
12.2(54)WO—Nov 29, 2010

These release notes describe the features, modifications, and caveats for Cisco IOS software on the Cisco Catalyst® 4948E-F Ethernet Switch.

Note Cisco IOS Release 12.2(54)WO is a rebuild of 12.2(54)SG, adding only hardware support for the Cisco Catalyst 4948E-F Ethernet Switch, which is a member of the Catalyst 4948E family of switches. This release is only supported on the Cisco Catalyst 4948E-F.

The Cisco Catalyst® 4948E and 4948E-F Ethernet Switches are the first Cisco Catalyst E-Series data switches built from the start to deliver class-leading full-featured server-access switching. Both switches offers forty-eight 10/100/1000-Gbps RJ45 downlink ports and four 1/10 Gigabit Ethernet uplink ports and are designed to simplify data center architecture and operations by offering enterprise grade hardware and software in a one rack unit (1 RU) form factor optimized for full-featured top-of-rack (ToR) data center deployments.

The Catalyst 4948E and 4948E-F share the same internal hardware and software. The Catalyst 4948E draws cold air into the port side and exhaust hot air at the power supply side. The Catalyst 4948E-F draws cold air at the power supply side and exhaust hot air at the port side. This is the only difference between the 4948E and 4948E-F.

The Cisco Catalyst 4948E family builds on the technology of the Cisco Catalyst 4948 Switches, the most deployed ToR switch in the industry, with more than 10 million ports deployed worldwide.

Characteristics of the Cisco Catalyst E-Series include:

- Forty-eight 10/100/1000-Gbps RJ45 downlink ports and four 1/10 Gigabit Ethernet uplink ports
- Doubled uplink bandwidth relative to the Catalyst 4948 switch
- True front-to-back and back-to-front airflow with no side or top venting, reducing data center operating costs by providing strict hot-aisle and cold-aisle isolation

  The Catalyst 4948E directs air from the port side to the power supply side of the chassis. The Catalyst 4948E-F directs air from the power supply side to the port side of the chassis.

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

- Very high reliability and serviceability through optional internal AC and DC 1+1 hot-swappable power and hot-swappable fan tray with redundant fans

Support for Cisco IOS Software Release 12.2(54)WO, the default image, follows the standard Cisco Systems® support policy, available at http://www.cisco.com/en/US/products/products_end-of-life_policy.html

For more information about the Cisco Catalyst 4948E Ethernet Switch, visit: http://www.cisco.com/go/cat4900/docs.

Contents

This publication consists of these sections:

Cisco IOS Software Packaging for the Cisco Catalyst 4948E-F Ethernet Switch

The Cisco Catalyst 4948E supports three levels of Cisco IOS Software, summarized in Table 1. The basic level is LAN Base, developed for deployments that require data center-grade hardware along with Layer 2 switching but not advanced features such as routing and Cisco IOS EEM. The next level of software is IP Base; most customers will deploy this level of software because it offers many of the Cisco value-added features that provide operational consistency and an easy-to-manage environment. The top level of software is Enterprise Services. Enterprise Services adds support for advanced routing protocols such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and Enhanced Interior Gateway Routing Protocol (EIGRP).

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

The following table lists the software configuration options.

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base	Enterprise Services
10G Uplink Use	Yes	Yes	Yes
802.1p prioritization	Yes	Yes	Yes
802.1p/802.1q	Yes	Yes	Yes
802.1w/802.1s	Yes	Yes	Yes
802.1X (w/ Guest VLAN and VLAN Assignment)	Yes	Yes	Yes
802.1X and MAB with ACL assignment	Yes	Yes	Yes
802.1X (Auth-Fail VLAN, Critical Auth, Accounting)	Yes	Yes	Yes
802.1X Wake on LAN	Yes	Yes	Yes
802.1X Web-Auth	Yes	Yes	Yes
802.1X with Multiple authenticated, multi-host	Yes	Yes	Yes
802.1X w/ MDA	Yes	Yes	Yes
802.1X w/ Open Access	Yes	Yes	Yes
802.3ad LACP	Yes	Yes	Yes
802.3x – Flow Control	Yes	Yes	Yes
ACL Logging	Yes	Yes	Yes
All Mibs	Yes	Yes	Yes
Auto QoS	Yes	Yes	Yes
Auto SmartPort	Yes	Yes	Yes
Auto-MDIX	Yes	Yes	Yes
Auto-Voice VLAN (part of Auto QoS)	No support	Yes	Yes
BOOTP	Yes	Yes	Yes
Bootup GOLD	No support	Yes	Yes
Broadcast Suppression	Yes	Yes	Yes
CDP/CDPv2	Yes	Yes	Yes
Community PVLAN support	No support	Yes	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base	Enterprise Services
Config File	Yes	Yes	Yes
Console Access	Yes	Yes	Yes
Control Plane Policing	Yes	Yes	Yes
Copy Command	Yes	Yes	Yes
CoS to DSCP Map	Yes	Yes	Yes
Debug Commands	Yes	Yes	Yes
Device Management	Yes	Yes	Yes
DHCP Server	Yes	Yes	Yes
DHCP Snooping	Yes	Yes	Yes
Diagnostics Tools	Yes	Yes	Yes
Downloading Software	Yes	Yes	Yes
DSCP to CoS Map	Yes	Yes	Yes
DSCP to egress queue mapping	Yes	Yes	Yes
Dynamic ARP inspection	Yes	Yes	Yes
EEM and EOT integration	Yes	No	Yes
EIGRP Stub	No support	Yes	Yes
EnergyWise 2.0	Yes	Yes	Yes
Event Log	Yes	Yes	Yes
Factory Default Settings	Yes	Yes	Yes
File Management	Yes	Yes	Yes
Flex Link	Yes	Yes	Yes
GLBP	No support	Yes	Yes
HSRP v1	No support	Yes	Yes
HSRP v2 IPV4[1]	No support	Yes	Yes
HSRP v2 IPV6[2]	No support	No	Yes
ID 4.0 Voice Vlan assignment	Yes	Yes	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base	Enterprise Services
ID4.1 Filter ID and per use ACL	Yes	Yes	Yes
IGMP	Yes	Yes	Yes
IGMP Snooping	Yes	Yes	Yes
Ingress Policing	Yes	Yes	Yes
Interface Access (Telnet, Console/Serial, Web)	Yes	Yes	Yes
IP Source Guard	Yes	Yes	Yes
IP Multicast	No support	Yes	Yes
IPV6 reformation	NA	Yes	Yes
IPV6 MLD snooping V1 and V2	Future	Yes	Yes
IPV6 Router Advertisement (RA) Guard	Yes	Yes	Yes
ISL Trunk	Yes	Yes	Yes
ISSU	No support	Yes	Yes
Jumbo Frames	Yes	Yes	Yes
Layer 2 Debug	Yes	Yes	Yes
Layer 2 PT and QinQ	No support	Yes	Yes
Layer 2 Traceroute	Yes	Yes	Yes
Link State Tracking	Yes	Yes	Yes
LLDP/LLDP-MED	Yes	Yes	Yes
LLDP enhancements (PoE+Layer 2 COS)	Yes	No	Yes
Local Web Auth	Yes	Yes	Yes
MAB (MAC Authentication Bypass)	Yes	Yes	Yes
MAC Address Filtering	Yes	Yes	Yes
MAC Based Access List	Yes	Yes	Yes
Management IPV6 port	Yes	Yes	Yes
MLD Snooping	Yes	Yes	Yes
Multicast Filtering	Yes	Yes	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base	Enterprise Services
Multihop SXP (CTS)	No support	Yes	Yes
Network Edge Authentication Topology (NEAT)	Yes	No	Yes
No. of QoS Filters No. of Security ACE	Yes (4K entries)	Yes	Yes
OSPF for Routed Access[3]	No support	Yes	Yes
PAgP	Yes	Yes	Yes
Passwords Password clear protection	Yes	Yes	Yes
PIM SM/DM	No support	Yes	Yes
Port Monitoring (interface Stats)	Yes	Yes	Yes
Port Security	Yes	Yes; only 1024 MACs	Yes
Post Status	Yes	Yes	Yes
PVST+	Yes	Yes	Yes
Q-in-Q	No support	Yes	Yes
RACL (DSCP based)	Yes	Yes	Yes
RADIUS/TACACS+ (AAA)	Yes	Yes	Yes
RMON	Yes	Yes	Yes
Routing – RIP, Static	Yes	Yes	Yes
RPR	Yes	Yes	Yes
RPVST+	Yes	Yes	Yes
RSPAN	Yes	Yes	Yes
Service Advertisement Framework (SAF)	Yes	Yes	Yes
Smart Call Home	No support	Yes	Yes
SmartPorts (Role based MACRO)	Yes	Yes	Yes
SNMP (including SNMv3)	Yes	Yes	Yes
Source port Filtering (Private VLAN)	Yes	Yes	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base	Enterprise Services
SPAN (# of sessions) – Port Mirroring	Yes (2 sessions)	Yes (8 bidirectional sessions)	Yes
SSHv2/Secure Copy, FTP, SSL, Syslog, Sys Information	Yes	Yes	Yes
Storm Control	Yes	Yes	Yes
TDR	No support	Yes	Yes
Time Protocols (SNTP, TimeP)	Yes	Yes	Yes
Time-based ACL	Yes	Yes	Yes
Traffic Mirroring (SPAN)	Yes	Yes	Yes
Trusted Boundary (LLDP & CDP Based)	Yes	Yes	Yes
UDLD	Yes	Yes	Yes
VACL and PACL	Yes	Yes	Yes
VLAN Mapping (VLAN Translation)	Yes	Yes	Yes
Voice VLAN	Yes	Yes	Yes
VRRP	No support	Yes	Yes
VTP	Yes	Yes	Yes
WCCP	No support	Yes	Yes
XML-PI	Yes	Yes	Yes

1. Supported on all supervisor engines.
2. Supported only for Catalyst 4900M and Supervisor Engines 6-E/6L-E.
3. Supported on WS-X45-SUP6-E and WS-X45-SUP6L-E

Orderable Product Numbers:

- S49ELB-12254WO(=)—Cisco IOS Software for Cisco Catalyst 4948E-F Series Switches (LAN Base image)
- S49ELBK9-12254WO(=)—Cisco IOS Software for Cisco Catalyst 4948E-F Series Switches (LAN Base image with Triple Data Encryption)
- S49EIPB-12254WO(=)—Cisco IOS Software for Cisco Catalyst 4948E-F Series Switches (IP Base image)
- S49EIPBK9-12254WO(=)— Cisco IOS Software for Cisco Catalyst 4948E-F Series Switches (IP Base image with Triple Data Encryption)
- S49EES-12254WO(=)—Cisco IOS Software for Cisco Catalyst 4948E-F Series Switches (Enterprise Services image with BGP support)

- S49EESK9-12254WO—Cisco IOS Software for Cisco Catalyst 4948E-F Series Switches (Enterprise Services image with Triple Data Encryption) and BGP support)
- WS-C4900-SW-LIC—Catalyst 4948E-F IP Base Upgrade License for LAN Base IOS

Support

Support for Cisco IOS Software Release 12.2(54)WO follows the standard Cisco Systems® support policy, available at
http://www.cisco.com/en/US/products/products_end-of-life_policy.html

System Requirements

This section describes the system requirements:

- Supported Hardware, page 8
- Supported Features, page 10

Supported Hardware

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

Table 2 Supported Hardware

Product Number (append with "=" for spares)	**Product Description**
Switch Chassis	
WS-C4948E-F	Cat 4948E-F, opt sw, 48-Port 10/100/1000 + 4 SFP/SFP+, no p/s, Fr Ext
WS-C4948E-F-S	Cat 4948E-F, IPB, 48-Port 10/100/1000+ 4 SFP/SFP+, AC p/s, Fr Ext
WS-C4948E-F-E	Cat 4948E-F, ES, 48-Port 10/100/1000+ 4 SFP/SFP+, AC p/s, Fr Ext
WS-C4948E-BDL	Green Bundle 10x WS-C4948E-F
Power Module	
PWR-C49E-300AC-F=	Cat 4948E-F 300W AC Power Supply Front exhaust
PWR-C49E-300AC-F/2	Cat 4948E-F 300W AC Power Supply Front exhaust redundant
Small Form-Factor Pluggable Modules.	
GLC-BX-D	1000BASE-BX10-D small form-factor pluggable module For DOM support, see Table 4 on page 9.
GLC-BX-U	1000BASE-BX10-U small form-factor pluggable module For DOM support, see Table 4 on page 9.bv
GLC-SX-MM	1000BASE-SX small form-factor pluggable module
GLC-LH-SM	1000BASE-LX/LH small form-factor pluggable module
GLC-ZX-SM	1000BASE-ZX small form-factor pluggable module
GLC-T	1000BASE-T small form-factor pluggable module

Table 2 Supported Hardware (continued)

Product Number (append with "=" for spares)	**Product Description**
CWDM-SFP-xxxx	CWDM small form-factor pluggable module (See Table 3 on page 9 for a list of supported wavelengths.) For DOM support, see Table 4 on page 9.
SFP+ Modules	
SFP-10G-SR	Cisco 10GBASE-SR SFP+ Module for MMF
SFP-10G-LR	Cisco 10GBASE-LR SFP+ Module for SMF
SFP-10G-LRM	Cisco 10GBASE-LRM SFP+ Module for MMF
SFP-H10GB-CU1M	10GBASE-CU SFP+ Cable 1 Meter
SFP-H10GB-CU3M	10GBASE-CU SFP+ Cable 3 Meter
SFP-H10GB-CU5M	10GBASE-CU SFP+ Cable 5 Meter
Other Modules	
WS-X4994	Blank PS Cover
WS-X4994=	Blank PS Cover Spare
WS-X4993-F=	Catalyst 4948E-F spare fan tray front exhaust, Spare
Green Bundles	
WS-C4948E-F-BDL	Green Bundle 10x WS-C4948E-F
WS-C4948E-F-BDL-1	Green Bundle 10x WS-C4948E-F

Table 3 briefly describes the supported wavelengths in the Catalyst 4948E-F series switches.

Table 3 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
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

Table 4 DOM Support on the Catalyst 4500 Series Switch

Transceiver Module	**Support in Software Since...**
DWDM-X2-*xx*	12.2(50)SG

Table 4 DOM Support on the Catalyst 4500 Series Switch

Transceiver Module	Support in Software Since...
GLC-BX-D	12.2(20)EWA
GLC-BX-U	12.2(20)EWA
DWDM-GBIC-*xx*	12.1(19)EW
CWDM- SFP-*xx*	12.2(20)EWA

The following tables lists the hardware supported on the Catalyst 4948E-F series switch.

Supported Features

Table 5 lists the Cisco IOS software features for the Cisco Catalyst 4948E-F Ethernet Switch.

Table 5 Cisco IOS Software Feature Set for the Cisco Catalyst 4948E-F Ethernet 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 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
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

Table 5 Cisco IOS Software Feature Set for the Cisco Catalyst 4948E-F Ethernet Switch

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
MAC Move and Replace
802.1X with Guest VLANs
802.1X with MAC Authentication Bypass
802.1X with Web-Based Authentication
802.1X with Inaccessible Authentication Bypass
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
Private VLANs
Private VLAN DHCP snooping
Private VLAN trunks
IEEE 802.1Q-based VLAN encapsulation
Multiple VLAN access port
VLAN Trunking Protocol (VTP) and VTP domains
VTP v3
Support for 4096 VLANs per switch
Unidirectional link detection (UDLD) and aggressive UDLD
Sub-second UDLD (Fast UDLD)
SNMP V3 support for Bridge-MIB with VLAN indexing
Ethernet CFM
Ethernet OAM Protocol
Supported Protocols

Table 5 Cisco IOS Software Feature Set for the Cisco Catalyst 4948E-F Ethernet Switch

DTP[4]
RIPv1[5] and RIPv2, Static Routing
EIGRP[6]
EIGRP Stub Routing
EIGRP Service Advertisement Framework[7]
OSPF[8]
BGP4[9]
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]
STP - Portfast BPDU Guard
STP- BPDU Filtering
STP - Root Guard
SCP[15]
Resilient Ethernet Protocol (REP)
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
Routed Jumbo Frame support
SPAN CPU port mirroring

Table 5 Cisco IOS Software Feature Set for the Cisco Catalyst 4948E-F Ethernet Switch

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)
CDP 2nd Port Status TLV
FlexLink and MAC Address-Table Move Update
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
VRRP
IGMP[17] snooping version1, version 2, and version 3 (Full Support)
IGMP filtering
IGMP Querier
Multicast VRF-lite
VRF-aware IP services
VRF-aware TACACS+
Configurable IGMP Leave Timer
Multicast Source Discovery Protocol (MSDP)
Smartports I custom macros
Smartports II default macros
Smartports III global macros
AutoSmart Port macro
Port Aggregation Protocol (PagP)
802.3ad LACP
SSH version 1 and version 2[18]
show interface capabilities command
Enhanced SNMP MIB support
SNMP[19] version 1, version 2, and version 3
SNMP version 3 (with encryption)
DHCP server and relay-agent

Table 5 Cisco IOS Software Feature Set for the Cisco Catalyst 4948E-F Ethernet Switch

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
ARP QoS
QoS for IPv6
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)
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)

Table 5 Cisco IOS Software Feature Set for the Cisco Catalyst 4948E-F Ethernet Switch

Per-VLAN Control Traffic Intercept
Table Map Based Classification
Interface Index Persistence
UDI - Unique Device Identifier
Per-port QoS[23] rate-limiting and shaping
Per-port Per-VLAN QoS
Energy Wise 2.0
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]
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
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

Table 5 Cisco IOS Software Feature Set for the Cisco Catalyst 4948E-F Ethernet Switch

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
Bidirectional PIM
OSPF and EIGRP Fast Convergence
Inactivity Timer
boot config command
Crashdump enhancement
Unicast MAC filtering
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
802.1Q Tunneling
VLAN Mapping (VLAN Translation)
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
IPSG for Static Hosts
XML Programmatic Interface

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.

Minimum and Recommended ROMMON Release

Table 6 Minimum and Recommended ROMMON Release for Catalyst 4948E-F

Minimum ROMMON Release	Recommended ROMMON Release
12.2(44r)SG9	12.2(44r)SG9

Limitations and Restrictions

Following limitations and restrictions apply to the Cisco Catalyst 4948E-F Ethernet Switch:

- 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 27 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 4948E-F switch.
- For PVST and Catalyst 4948E-F switch VLANs, Cisco IOS Release 12.2(54)WO 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-F 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-F 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.
- 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.
- The Cisco IOS Release 12.2(54)WO releases supports 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-F 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 4948E-F switchport. IPv6 packets cannot be filtered on switchports using any of the known methods (PACL, VACL, or MACLs).
- Class-map match statements using **match ip prec | dscp** match only IPv4 packets whereas matches performed with **match prec | dscp** match both IPv4 and IPv6 packets.
- IPv6 QoS hardware switching is disabled if the policy-map contains IPv6 ACL and match cos in the same class-map with the ipv6 access-list has any mask 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(54)WO.
- 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.
- The Catalyst 4948E-F Ethernet Switch upstream ports support flow control auto negotiation in 1G mode only, and flow control is forced in 10G mode. If the interface is configured to auto-negotiate the flow control, and the interface is operating in 10G mode, the system forces flow control to ON and does not auto-negotiate.
- 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-F Ethernet switch supports fast UDLD on a maximum of 32 ports.

Caveats

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

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

Open Caveats in Cisco IOS Release 12.2(54)WO

This section lists the open caveats in Cisco IOS Release 12.2(54)WO:

- 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.

- 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)

- 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)

- If VLAN Load Balancing is progressing, and you reconfigure VLAN Load Balancing to reflect different blocking ports, manual preemption does not occur.

  Workaround: To reconfigure VLAN Load Balancing with a different configuration, do the following:

  a. Reconfigure the VLAN Load Balancing configuration on the desired REP ports.
  b. **Shut** any one REP port in the segment to cause a failure in that segment.
  c. **No-shut** that port to restore normal REP topology with one ALT port.
  d. Invoke manual preemption on a primary edge port to obtain VLAN Load Balancing with the new configuration.

  (CSCsv69853)

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

  Workaround: None. CSCsy72343

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

  Workaround: None.

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

  CSCsz20149

- When you configure **switchport block multicast** on a switch running Cisco IOS Release 12.2(54)WO, Layer 2 multicast is not blocked.

  Workaround: None

  CSCtb30327

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

  This occurs only if the following conditions are satisfied:

  - Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
  - Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
  - Dynamic policy authorization for the client specifies **permit ip any any**.

  Workaround: None.

  CSCsz63739

- If *time* is not specified in the **link debounce** command, the default value is 100 ms.

  Workaround: None.

  CSCte51948

- High CPU usage results when around 1000 secondary VLANs are mapped to the primary VLAN SVI.

  Workaround: None. CPU usage will decrease after some time.

  CSCtc30070

- When **ipv6 nd raguard** is configured on an interface, Router Advertisement and Router Redirect packets with destination address FF02::x are dropped as expected. However, the drop counters are not advanced in the output of **show ipv6 first-hop counters** *interface* interface command.

  Workaround: None. CSCtf69108

- On a peer interface, 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

- 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

- 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)

- Occasionally, when you use MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1
   Service-policy output: p1
     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

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

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

  Workaround: Reconnect. (CSCsb11964)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port. This situation could occur for these reasons:
  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of bootup.
  - The administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

  Workarounds:
  - Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. CSCse75660
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

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

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. CSCsg27395
- Occassionally, when a transceiver is quickly removed from a port and placed in another port on the same chassis, a duplicate seeprom message appears and the port is unable to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. CSCse34693
- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

  Workaround: None. (CSCsm30320)
- An IP unnumbered configuration is lost after a switch reloads.

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

  CSCsq63051
- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

  Workaround: Configure an ISL or 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 or earlier.

Workaround: None. (CSCsw14005)

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk port. However, the traffic is properly classified and the actions configured in the policy are applied properly.

  Workaround: None. CSCsy72343

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

  Workaround: None.

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

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

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

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

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

  CSCsz34522

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

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

  Workaround: None. CSCtb30327

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

  Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

  a. Reconfigure the VLAN load balancing configuration on the desired REP ports.
  b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
  c. Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
  d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration. CSCsv69853

- On a peer interface for 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 switch default link-flap detection value is 5 flaps in 10 seconds. Use the default value or larger numbers. CSCtg07677

- If you disable and re-enable IGMP Snooping on a VLAN, the output of the **show mac address** command does not display the [term] Switch against the multicast entry. Multicast traffic is not impacted.

  Workaround: Enter **shut** then **no shut** on the SVI. CSCtg72559

- When a connected data device behind a phone disconnects from a port configured for multi-auth host mode, a new session for the device is restarted even though the device is absent.

  The CDP TLV generated to indicate that a data device has disconnected is ignored. This is done to avoid disconnecting other connected data clients, if any. (Refer to CSCta47293.)

  Workarounds: Enter either of the following commands:

  – **clear authentication session interface**

  – **authentication timer inactivity** CSCtg83631

- When Fallback WebAuth and Multi-host are configured on a port and no PACL exists, **permit ip any any** is installed in the TCAM and all traffic from the host is allowed to pass.

  Workaround: Configure an ACL on the port. CSCte18760

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

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

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

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

  Workaround: None. (CSCso93282)

- A switch may crash while loading BGP routes if the **ip cef accounting non-recursive** command is already configured.

  Workaround: Disable the **ip cef accounting non-recursive** command.

  (CSCtn68186)

Resolved Caveats in Cisco IOS Release 12.2(54)WO

This section lists the resolved caveats in Cisco IOS Release 12.2(54)WO:

- The SFP+ interfaces on Catalyst 4948E Ethernet Switch , Supervisor 7, Supervisor 7-E, and WS-X4712-SFP+E auto-detect the presence of 10 Gigabut or 1 Gigabut-optics and set the speed automatically. However, in Cisco IOS Releases IOS-XE 3.1.0SG, 12.2(54)XO, and 12.2(54)SG, CLI speed nonegotiate does not actually turn off the speed negotiation with the peer. This means that if the peer does not negotiate speed, the interfaces will not link up.

  Workaround: Apply auto negotiation on the peer.

  Issue resolved in Cisco IOS Release 15.0(2)SG.

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 the 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/US/products/hw/switches/ps4324/prod_installation_guides_list.html

- *Regulatory Compliance and Safety Information for the Catalyst 4500 Series Switches*

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/regulatory/compliance/78_13233.html

- Installation notes for specific supervisor engines or for accessory hardware are available at:

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

- Catalyst 4900 and 4900M hardware installation information is available at:

  http://www.cisco.com/en/US/products/ps6021/prod_installation_guides_list.html

- Cisco ME 4900 Series Ethernet Switches installation information is available at:

  http://www.cisco.com/en/US/products/ps7009/prod_installation_guides_list.html

Software Documentation

Software release notes, configuration guides, command references, and system message guides are available at the following URLs:

- Catalyst 4500 release notes are available at:

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

- Catalyst 4900 release notes are available at:

  http://www.cisco.com/en/US/products/ps6021/prod_release_notes_list.html

- Cisco ME4900 4900 Series Ethernet Switch release notes are available at:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_11511.html

Software documents for the Catalyst 4500 Classic, Catalyst 4500 E-Series, Catalyst 4900, and Cisco ME 4900 Series Ethernet Switches are available at the following URLs:

- *Catalyst 4500 Series Software Configuration Guide*

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

- *Catalyst 4500 Series Software Command Reference*

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

- *Catalyst 4500 Series Software System Message Guide*

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

Cisco IOS Documentation

Platform-independent Cisco IOS documentation may also apply to the Catalyst 4500 and 4900 switches. These documents are available at the following URLs:

- Cisco IOS configuration guides, Release 12.x

  http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html

- Cisco IOS command references, Release 12.x

  http://www.cisco.com/en/US/products/ps6350/prod_command_reference_list.html

  You can also use the Command Lookup Tool at:

http://tools.cisco.com/Support/CLILookup/cltSearchAction.do

- Cisco IOS system messages, version 12.x

  http://www.cisco.com/en/US/products/ps6350/products_system_message_guides_list.html

  You can also use the Error Message Decoder tool at:

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

- For information about MIBs, refer to:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

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

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

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

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

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

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

Original SSLeay License:

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

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

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

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

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

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

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

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

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

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT

NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Obtaining Documentation and Submitting a Service Request

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

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

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

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

Release Notes for the Catalyst 4900 Series Switch, Cisco IOS Release 12.2(54)WO