Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Releases 12.2(25)EWA to 12.1(8a)EW

Current Release
12.2(54)SG1—February 7, 2011

Previous Releases
12.2(25)EWA14, 12.2(25)EWA13, 12.2(25)EWA12, 12.2(25)EWA11, 12.2(25)EWA10, 12.2(25)EWA9, 12.2(25)EWA8, 12.2(25)EWA7, 12.2(25)EWA6, 12.2(25)EWA5, 12.2(25)EWA4, 12.2(25)EWA3, 12.2(25)EWA2, 12.2(25)EWA1, 12.2(25)EW, 12.2(20)EWA4, 12.2(20)EWA3, 12.2(20)EWA2, 12.2(20)EWA1, 12.2(20)EWA, 12.2(20)EW4, 12.2(20)EW3, 12.2(20)EW2, 12.2(20)EW1, 12.2(20)EW, 12.2(18)EW7, 12.2(18)EW6, 12.2(18)EW5, 12.2(18)EW4, 12.2(18)EW3, 12.2(18)EW2, 12.2(18)EW1, 12.2(18)EW, 12.1(20)EW4, 12.1(20)EW3, 12.1(20)EW1, 12.1(20)EW, 12.1(19)EW3, 12.1(19)EW2, 12.1(19)EW1, 12.1(19)EW, 12.1(13)EW4, 12.1(13)EW3, 12.1(13)EW1, 12.1(13)EW, 12.1(12c)EW4, 12.1(12c)EW3, 12.1(12c)EW1, 12.1(12c)EW, 12.1(11b)EW1, 12.1(11b)EW, 12.1(8a)EW1, 12.1(8a)EW

Orderable Product Numbers:

- S4KL3-12225EWA—Cisco IOS software for the Catalyst 4500 series switch, basic Layer 3 and voice software image (RIPv1, RIPv2, Static Routes, AppleTalk, and IPX Software Routing, Release 12.2(25)EWA (cat4000-i9s-mz.122-25.EWA)

Note We recommend that you load 12.2(31)SGA8.

- S4KL3E-12225EWA—Cisco IOS software for the Catalyst 4500 series switch, enhanced Layer 3 and voice software image including OSPF, IS-IS, and EIGRP, Release 12.2(25)EWA (cat4000-i5s-mz.122-25.EWA)
- S4KL3K9-12225EWA—Cisco IOS software for the Catalyst 4500 series switch, with 3DES strong encryption, basic Layer 3 and voice software image (SSHv1, SSHv2, RIPv1, RIPv2, static routes, AppleTalk, and IPX), Release 12.2(25)EWA (cat4000-i9k9s-mz.122-25.EWA)
- S4KL3EK9-12225EWA—Cisco IOS software for the Catalyst 4500 series switch, with 3DES strong encryption, enhanced Layer 3 and voice software image including (OSPF, IS-IS, IGRP, and EIGRP), Release 12.2(25)EWA (cat4000-i5k9s-mz.122-25.EWA)

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

- S4KL3-12220EWA—Cisco IOS software for the Catalyst 4500 series switch, basic Layer 3 and voice software image (RIPv1, RIPv2, Static Routes, AppleTalk, and IPX Software Routing, Release 12.2(20)EWA (cat4000-i9s-mz.122-20.EWA)
- S4KL3E-12220EWA—Cisco IOS software for the Catalyst 4500 series switch, enhanced Layer 3 and voice software image including OSPF, IS-IS, and EIGRP, Release 12.2(20)EWA (cat4000-i5s-mz.122-20.EWA)
- S4KL3K9-12220EWA—Cisco IOS software for the Catalyst 4500 series switch, with 3DES strong encryption, basic Layer 3 and voice software image (SSHv1, SSHv2, RIPv1, RIPv2, static routes, AppleTalk, and IPX), Release 12.2(20)EWA (cat4000-i9k9s-mz.122-20.EWA)
- S4KL3EK9-12220EWA—Cisco IOS software for the Catalyst 4500 series switch, with 3DES strong encryption, enhanced Layer 3 and voice software image including (OSPF, IS-IS, IGRP, and EIGRP), Release 12.2(20)EWA (cat4000-i5k9s-mz.122-20.EWA)
- S4KL3-12220EW—Cisco IOS software for the Catalyst 4500 series switch, basic Layer 3 and voice software image (RIPv1, RIPv2, Static Routes, AppleTalk, and IPX), Release Software Routing, Release 12.2(20)EW (cat4000-i9s-mz.122-20.EW)
- S4KL3E-12220EW—Cisco IOS software for the Catalyst 4500 series switch, enhanced Layer 3 and voice software image including OSPF, IS-IS, and EIGRP, Release 12.2(20)EW (cat4000-i5s-mz.122-20.EW)
- S4KL3K91-12220EW—Cisco IOS software for the Catalyst 4500 series switch, with 3DES strong encryption, basic Layer 3 and voice software image (SSHv1, SSHv2, RIPv1, RIPv2, static routes, AppleTalk, and IPX), Release 12.2(20)EW (cat4000-i9k91s-mz.122-20.EW)
- S4KL3EK91-12220EW—Cisco IOS software for the Catalyst 4500 series switch, with 3DES strong encryption, enhanced Layer 3 and voice software image including (OSPF, IS-IS, and EIGRP), Release 12.2(20)EW (cat4000-i5k91s-mz.122-20.EW)
- S4KL3-12218EW—Cisco IOS software for the Catalyst 4500 series switch, basic Layer 3 and voice software image (RIPv1, RIPv2, Static Routes, AppleTalk, and IPX), Release Software Routing, Release 12.2(18)EW (cat4000-i9s-mz.122-18.EW)
- S4KL3E-12218EW—Cisco IOS software for the Catalyst 4500 series switch, enhanced Layer 3 and voice software image including OSPF, IS-IS, and EIGRP, Release 12.2(18)EW (cat4000-i5s-mz.122-18.EW)
- S4KL3K91-12218EW—Cisco IOS software for the Catalyst 4500 series switch, with 3DES strong encryption, basic Layer 3 and voice software image (SSHv1, SSHv2, RIPv1, RIPv2, static routes, AppleTalk, and IPX), Release 12.2(18)EW (cat4000-i9k91s-mz.122-18.EW)
- S4KL3EK91-12218EW—Cisco IOS software for the Catalyst 4500 series switch, with 3DES strong encryption, enhanced Layer 3 and voice software image including (OSPF, IS-IS, and EIGRP), Release 12.2(18)EW (cat4000-i5k91s-mz.122-18.EW)
- S4KL3-12120EW—Cisco IOS software for the Catalyst 4500 series switch, basic Layer 3 and voice software image (RIPv1, RIPv2, Static Routes, AppleTalk, and IPX), Release Software Routing, Release 12.1(20)EW (cat4000-i9s-mz.121-20.EW)
- S4KL3E-12120EW—Cisco IOS software for the Catalyst 4500 series switch, Supervisor Engines III and IV, enhanced Layer 3 and voice software image including OSPF, IS-IS, IGRP, and EIGRP, Release 12.1(20)EW (cat4000-i5s-mz.121-20.EW)
- S4KL3K2-12120EW—Cisco IOS software for the Catalyst 4500 series switch, with 3DES strong encryption, basic Layer 3 and voice software image (SSHv1, SSHv2, RIPv1, RIPv2, static routes, AppleTalk, and IPX), Release 12.1(20)EW (cat4000-i9k2s-mz.121-20.EW)

- S4KL3EK2-12120EW—Cisco IOS software for the Catalyst 4500 series switch, Supervisor Engines III and IV with 3DES strong encryption, enhanced Layer 3 and voice software image including (OSPF, IS-IS, IGRP, and EIGRP), Release 12.1(20)EW (cat4000-i5k2s-mz.121-20.EW)
- S4KL3-12119EW—Cisco IOS software for the Catalyst 4500 series switch, basic Layer 3 and voice software image (RIPv1, RIPv2, Static Routes, AppleTalk, and IPX), Release Software Routing, Release 12.1(19)EW (cat4000-i9s-mz.121-19.EW)
- S4KL3E-12119EW—Cisco IOS software for the Catalyst 4500 series switch, Supervisor Engines III and IV, enhanced Layer 3 and voice software image including OSPF, IS-IS, IGRP, and EIGRP, Release 12.1(19)EW (cat4000-i5s-mz.121-19.EW)
- S4KL3K2-12119EW—Cisco IOS software for the Catalyst 4500 series switch with 3DES strong encryption, basic Layer 3 and voice software image (SSHv1, SSHv2, RIPv1, RIPv2, static routes, AppleTalk, and IPX), Release 12.1(19)EW (cat4000-i9k2s-mz.121-19.EW)
- S4KL3EK2-12119EW—Cisco IOS software for the Catalyst 4500 series switch, Supervisor Engines III and IV with 3DES strong encryption, enhanced Layer 3 and voice software image including (OSPF, IS-IS, IGRP, and EIGRP), Release 12.1(19)EW (cat4000-i5k2s-mz.121-19.EW)
- S4KL3-12113EW—Cisco IOS software for the Catalyst 4500 series switch, Supervisor Engines III and IV, basic Layer 3 and voice software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(13)EW
- S4KL3E-12113EW—Cisco IOS software for the Catalyst 4500 series switch, Supervisor Engines III and IV, enhanced Layer 3 and voice software image including OSPF, IGRP, EIGRP, and IS-IS, Release 12.1(13)EW
- S4KL3K2-12113EW—Cisco IOS software for the Catalyst 4500 series switch, Supervisor Engines III and IV with 3DES strong encryption, basic Layer 3 and voice software image (SSHv1, RIP, static routes, AppleTalk and IPX), Release 12.1(13)EW
- S4KL3EK2-12113EW—Cisco IOS software for the Catalyst 4500 series switch, Supervisor Engines III and IV with 3DES strong encryption, enhanced Layer 3 and voice software image including OSPF, IGRP, EIGRP, and IS-IS, Release 12.1(13)EW
- S4KL3-12112EW—Cisco IOS software for the Catalyst 4500 series switch, Supervisor Engines III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(12c)EW
- S4KL3E-12112EW—Cisco IOS software for the Catalyst 4500 series switch, Supervisor Engines III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(12c)EW
- S4KL3-12111EW—Cisco IOS software for the Catalyst 4500 series switch, basic Layer 3 software image (RIP, static routes), Release 12.1(11b)EW
- S4KL3E-12111EW—Cisco IOS software for the Catalyst 4500 series switch, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(11b)EW1
- S4KL3-12108EW—Cisco IOS software for the Catalyst 4500 series switch, basic Layer 3 software image (RIP, static routes), Release 12.1(8a)EW
- S4KL3E-12108EW—Cisco IOS software for the Catalyst 4500 series switch, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(8a)EW1

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(25)EWA

Release 12.2(25)EWA provides the following new hardware for the Catalyst 4500 series switch:

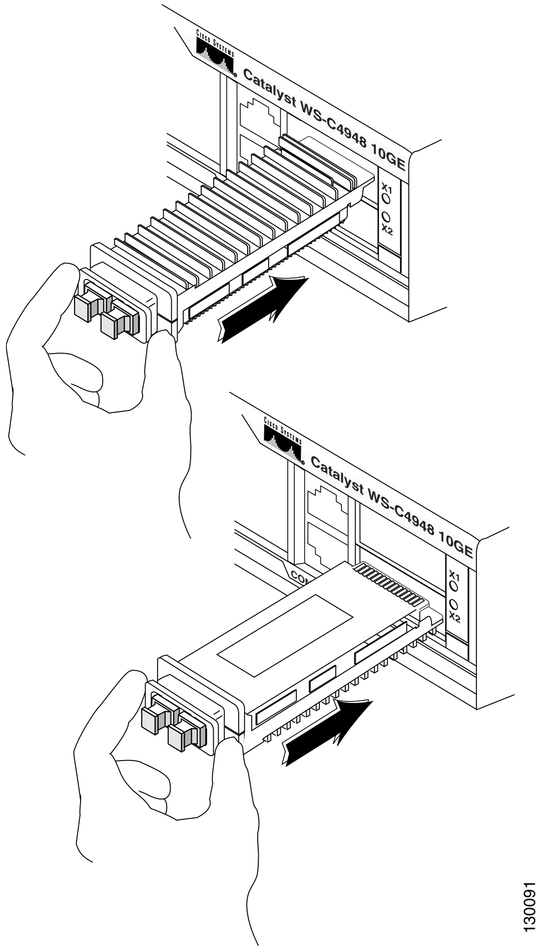
- WS-X4948-10GE—Catalyst 4948 48-Port 10/100/1000 + 2 10GE in a 1 RU with dual, redundant AC/DC power

If you plan to insert X2 transceivers in the Cisco Catalyst 4948-10GE, you should ensure that the Catalyst 4500 series switch and the X2 back interfaces are properly oriented during the OIR (Online insertion and removal) of the transceivers. The top transceiver (port tengig1/49) should be inserted with heatsink facing up. The bottom transceiver (port tengig1/50) should be plugged in with heatsink facing down, CLEI (Common Language Equipment Identifiers) label facing up. (See Figure 1.). When inserted correctly, the TX/RX of the bottom transceiver would look reversed. For more details refer to the *Catalyst 4900 Installation Guide*, at the URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4900/installation/guide/4900.html

- PWR-C45-4200ACV—Catalyst 4500 series switch 4200 Watt AC dual input power supply with integrated voice (data and PoE)

Figure 1 Cavities of X2 Transceivers on the Catalyst 4948-10GE



New Software Features in Release 12.2(25)EWA

Release 12.2(25)EWA 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*.

- Per-Port Per-VLAN QoS (“Configuring QoS and Per-Port Per-VLAN QoS” chapter)
- Trunk-Port Security (“Configuring Port Security and Trunk Port Security” chapter)
- NetFlow Bridged IP Flow (“Configuring NetFlow Statistics Collection” chapter)
- 802.1X Private VLAN Assignment (“Understanding and Configuring 802.1X Port-Based Authentication” chapter)

- 802.1X Private Guest VLAN ("Understanding and Configuring 802.1X Port-Based Authentication" chapter)
- 802.1X Radius-Supplied Session Timeout ("Understanding and Configuring 802.1X Port-Based Authentication" chapter)
- DHCP Option 82 Pass Through ("Configuring DHCP Snooping and IP Source Guard" chapter)
- Time-based ACL

New Hardware Features in Release 12.2(25)EW

Note This release is deferred to 12.2(25)EWA2.

Release 12.2(25)EW provides the following new hardware for the Catalyst 4500 series switch:

- WS-X4516-10GE—Catalyst 4500 series switch Supervisor Engine V-10GE
- PWR- C45-1400DC SP—Catalyst 4500 series switch 1400 DC triple input power supply (data-only)

New Software Features in Release 12.2(25)EW

Note This release is deferred to 12.2(25)EWA2.

Release 12.2(25)EW 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*.

- Enhanced NetFlow support on the Catalyst 4500 series switch Supervisor Engine V-10GE
- 10-Gigabit Ethernet support on the Catalyst 4500 series switch Supervisor Engine V-10GE

New Hardware Features in Release 12.2(20)EWA

Release 12.2(20)EWA provides the following new hardware for the Catalyst 4500 series switch:

- WS-X4013+TS—Catalyst 4500 series switch Supervisor Engine II-Plus-TS
- WS-X4506-GB-T—Catalyst 4500 series 6-Port Alternatively-Wired 10/100/1000 Power over Ethernet (PoE) or 1000BASE-X SFP module
- WS-X4948—Catalyst 4948 48-Port 10/100/1000 + 4 SFP in a 1 RU with dual, redundant AC/DC power

New Software Features in Release 12.2(20)EWA

Release 12.2(20)EWA 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*.

- Non-Stop Forwarding Awareness ("Configuring Supervisor Engine Redundancy Using RPR and SSO" chapter)
- Stateful Switchover ("Configuring Supervisor Engine Redundancy Using RPR and SSO" chapter)
- 802.1X with Voice VLAN ID ("Understanding and Configuring 802.1X Port-Based Authentication" chapter)
- Forced 10/100 Auto Negotiation ("Configuring Interfaces" chapter)
- PIM SSM for IGMPv2 using DNS or static mapping (IOS standard documentation)

New Hardware Features in Release 12.2(20)EW

Release 12.2(20)EW provides the following new hardware for the Catalyst 4500 series switch:

- WS-X4124-RJ45—Catalyst 4500 series 24-port 10/100(RJ-45) module
- WS-X4224-RJ45V—Catalyst 4500 series Power over Ethernet (PoE) 10/100-Mbps, 24-port (RJ-45) 802.3af
- WS-X4448-GB-SFP—Catalyst 4500 series 48-Port 1000BASE-X SFP module
- WS-X4524-GB-RJ45V—Catalyst 4500 series Power over Ethernet (PoE) 10/100/1000-Mbps, 24-port (RJ-45) 802.3af

New Software Features in Release 12.2(20)EW

Release 12.2(20)EW 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*.

- Community PVLAN ("Configuring Private VLANs" chapter)
- SPAN ACL Filtering ("Configuring SPAN and RSPAN" chapter)
- DHCP Client Autoconfiguration ("Configuring the Switch for the First Time" chapter)
- Software-based IPv6

For information on the IPv6 feature, refer to the following URL:

http://www.cisco.com/en/US/technologies/collateral/tk648/tk872/tk373/technologies_white_paper_09186a00802219bc.html

New Hardware Features in Release 12.2(18)EW

Release 12.2(18)EW provides the following new hardware for the Catalyst 4500 series switch:

- WS-X4516—Catalyst 4500 series switch Supervisor Engine V
- WS-C4510R—Catalyst 4500 series switch chassis with 10 slots (supports Supervisor Engine V only)
- WS-X4148-FE-BD-LC—Catalyst 4500 series switch 48-port 100BASE-BX10-D module
- WS-X4248-RJ45V—Catalyst 4500 series switch Power over Ethernet (PoE) 10/100-Mbps, 48 port (RJ-45)
- WS-X4248-RJ21V—Catalyst 4500 series switch Power over Ethernet (PoE) 10/100-Mbps, 48 port telco (4xRJ-21)
- WS-X4548-GB-RJ45V—Catalyst 4500 series switch Power over Ethernet (PoE) 48-port 10/100/1000-Mbps (RJ-45)

New Software Features in Release 12.2(18)EW

Release 12.2(18)EW 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*.

- 802.1Q Tunneling (Q in Q) (“Configuring 802.1Q and Layer 2 Protocol Tunneling” chapter)
- Layer 2 Protocol Tunneling (“Configuring 802.1Q and Layer 2 Protocol Tunneling” chapter)
- Storm Control (“Configuring Port-Based Traffic Control” chapter)
- Sticky Port Security (“Configuring Port Security” chapter)
- 802.1X with Port Security (“Understanding and Configuring 802.1X Port-Based Authentication” chapter)
- 802.1X Accounting (“Understanding and Configuring 802.1X Port-Based Authentication” chapter)
- SmartPort Macros (“Configuring SmartPort Macros” chapter)
- Chassis and Inline Power Management (“Environmental Monitoring and Power Management” chapter)

New Hardware Features in Release 12.1(20)EW

There are no new hardware features in Release 12.1(20)EW.

New Software Features in Release 12.1(20)EW

Release 12.1(20)EW provides the following Cisco IOS features for the Catalyst 4500 series switch:

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

- Internet Group Management Protocol (IGMP) v3 snooping enhancements ("Configuring IGMP Snooping and Filtering" chapter)
- Virtual Routing Forwarding-lite ("Configuring VRF-lite" chapter)
- Remote Switched Port ANalyzer ("Configuring SPAN and RSPAN" chapter)
- Pragmatic General Multicast (PGM)
- Port Security on PVLAN ports
- Dynamic ARP Inspection on PVLAN ports
- Authentication, authorization, and accounting using TACACS+ and RADIUS protocol
- Internetwork Packet Exchange (IPX)/AppleTalk access control lists (ACLs)
  - <1000-1099> IPX SAP access list
  - <800-899> IPX standard access list
  - <900-999> IPX extended access list
- Transceiver Optical Monitoring
- Enhanced Simple Network Management Protocol (SNMP) Management Information Base (MIB) support

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

New Hardware Features in Release 12.1(19)EW

Release 12.1(19)EW provides the following new hardware for the Catalyst 4500 series switch:

- WS-X4013+—Catalyst 4500 series Supervisor Engine II-Plus
- WS-X4548-GB-RJ45—Catalyst 4500 series 48-port 10/100/1000 RJ-45 line card
- WS-X4302-GB—Catalyst 4500 series 2-port Gigabit Ethernet line card
- DWDM-GBIC-xx.yy—Cisco DWDM GBICs
- WDM-GBIC-REC—Cisco receive-only 1000BASE-WDM GBIC

New Software Features in Release 12.1(19)EW

Release 12.1(19)EW 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*.

- Storm Control ("Configuring Port-Based Traffic Control" chapter)
- Per-VLAN Rapid Spanning Tree ("Understanding and Configuring STP" chapter)
- Trusted boundary ("Configuring QoS" chapter)
- Auto QoS ("Configuring QoS" chapter)
- Secure access with Secure Shell Protocol (SSHv2)
- **show interface capabilities** command ("Configuring Port-Based Traffic Control" chapter)
- NetFlow version 8 ("Configuring NetFlow Statistics Collection" chapter)
- Port ACL ("Configuring Network Security with ACLs" chapter)
- Dynamic ARP Inspection ("Understanding and Configuring Dynamic ARP Inspection" chapter)
- IP source guard ("Configuring DHCP Snooping and IP Source Guard" chapter)

Note For any network deployment of Dynamic ARP Inspection, IP Source Guard and the DHCP snooping features, it is essential that you read the white paper "Catalyst 4500 Security Services Best Practices" at the URL:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a00801b49a4.shtml

- CPU port sniffing ("Configuring SPAN" chapter)
- Packet type filtering ("Configuring SPAN" chapter)
- Ingress packets ("Configuring SPAN" chapter)
- Port flood blocking ("Port Unicast and Multicast Flood Blocking" chapter)
- 802.1X with VLAN assignment ("Configuring 802.1X Port-Based Authentication" chapter)
- 802.1X with guest VLAN ("Configuring 802.1X Port-Based Authentication" chapter)
- IGMP version 3 ("Configuring IGMP Snooping and Filtering" chapter)
- Unidirectional link routing ("Configuring Unidirectional Link Routing" chapter in the *Cisco IP and IP Routing Configuration Guide)*
- Inline power preallocation ("Environmental Monitoring and Power Management" chapter)
- IPX performance enhancements

  The delivery latency for IPX packet forwarding has been significantly improved. For lock-step based protocols with single or small packet window sizes, this results in an increased throughput rate and better responsiveness.

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

New Hardware Features in Release 12.1(13)EW

Release 12.1(13)EW provides the following new hardware for the Catalyst 4500 series switch:

- WS-F4531—Catalyst 4500 Series NetFlow Services Card
- WS-G5483—Cisco 1000BASE-T GBIC
- WS-X4604-GWY—Cisco Catalyst 4000 Access Gateway Module
- WS-X4148-FE-LX-MT—48-port 100BASE-LX10 Fast Ethernet switching module

New Software Features in Release 12.1(13)EW

Release 12.1(13)EW provides the following Cisco IOS software features for the Catalyst 4500 series switch:

- The new Layer 2 features are as follows:

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

  - VLAN Management Policy Server (VMPS) client (“Configuring Dynamic VLAN Membership” chapter)
  - Support for 9216 byte frames (“Configuring Interfaces” chapter)
  - Unicast MAC filtering (“Configuring Network Security with ACLs” chapter)
  - Layer 2 traceroute (“Checking Port Status and Connectivity” chapter)
  - Unidirectional Ethernet port (“Configuring Unidirectional Ethernet” chapter)
  - Private VLAN DHCP snooping (“Configuring PVLANs” chapter)
  - Port security (“Configuring Port Security” chapter)
- The new Layer 3 features are as follows:
  - PBR (policy-based routing) (“Configuring Policy-Based Routing” chapter)
  - Dynamic Buffer Limiting (“Understanding and Configuring QoS” chapter)
- Secure access via secure shell (SSH) Protocol
- Intermediate System to Intermediate System (IS-IS)
- NetFlow VLAN Statistics
- NetFlow Statistics Collection
- NetFlow Statistics Export Version 1 and Version 5
- IEEE 802.3ad (“Understanding and Configuring EtherChannel” chapter)
- Enhanced SNMP MIB support

For more information on these features, refer to these publications:

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

New Hardware Features in Release 12.1(12c)EW

Release 12.1(12c)EW provides the following new hardware for the Catalyst 4500 series switch:

- PWR-C45-1000AC—Catalyst 4500 1000 Watt AC Power Supply (data only)
- PWR-C45-2800AC—Catalyst 4500 2800 Watt AC Power Supply (with integrated voice)
- WS-C4503—Catalyst 4503 chassis with 3 slots and a fan
- WS-C4506—Catalyst 4506 chassis with 6 slots and a fan
- WS-C4507R—Cisco Catalyst 4507 chassis with 7 slots and a fan (supports Supervisor Engine IV only)
- WS-X4515—Cisco Catalyst 4500 Supervisor Engine IV
- WS-X4515/2—Cisco Catalyst 4507R Redundant Supervisor Engine IV
- CWDM-GBIC-1470—Longwave 1470 nm laser single-mode
- CWDM-GBIC-1490—Longwave 1490 nm laser single-mode
- CWDM-GBIC-1510—Longwave 1510 nm laser single-mode
- CWDM-GBIC-1530—Longwave 1530 nm laser single-mode
- CWDM-GBIC-1550—Longwave 1550 nm laser single-mode
- CWDM-GBIC-1570—Longwave 1570 nm laser single-mode
- CWDM-GBIC-1590—Longwave 1590 nm laser single-mode
- CWDM-GBIC-1610—Longwave 1610 nm laser single-mode

New Software Features in Release 12.1(12c)EW

Release 12.1(12c)EW provides the following Cisco IOS features for the Catalyst 4500 series switch.

- The new Layer 2 features are as follows:

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

  - Support for 4096 VLANs per switch (refer to the “Understanding and Configuring VLANs” chapter)
  - Support for 1600 byte-sized frames to enable two nested 802.1q headers (802.1q in 802.1q pass-through) and Multiprotocol Label Switching (MPLS) on the network (refer to the “Understanding and Configuring VLANs" chapter)
  - Spanning-tree Loop guard and PortFast BPDU Filtering (refer to the “Configuring STP Features” chapter)
  - 802.1s and 802.1w (refer to the “Understanding and Configuring Multiple Spanning Trees” chapter)
  - IGMP filtering on trunks
  - PVLAN isolated trunk port (refer to the “Configuring PVLANs” chapter)
  - DHCP snooping (refer to the “Understanding and Configuring DHCP Snooping" chapter)

  - 802.1X port-based authentication (refer to the "Configuring 802.1X Port-Based Authentication" chapter)
  - VLAN access control lists (refer to the "Configuring Network Security with ACLs" chapter)
- The new Layer 3 features are as follows:
  - Software routing IPX and Appletalk
- Supervisor Engine Redundancy (refer to the “Configuring Supervisor Engine Redundancy on the Catalyst 4507R” chapter)
- Support for SPAN sessions with both received and transmitted traffic (refer to the “Configuring SPAN” chapter)

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

New Hardware Features in Release 12.1(11b)EW

Release 12.1(11b)EW provides initial support of the Cisco IOS software for the Catalyst 4006 switch with Supervisor Engine III and the following modules:

- WS-X4148-RJ45V—48-port inline power 10/100BASE-TX switching module with inline power support
- WS-X4095-PEM—Catalyst 4000 DC Power Entry Module
- WS-P4603-2PSU—Catalyst 4000 Auxiliary Power Shelf (3-slot) including two WS-X4608 power supplies
- WS-X4608—Catalyst 4603 Power Supply Unit for WS-P4603

New Software Features in Release 12.1(11b)EW

Release 12.1(11b)EW provides initial support of the Cisco IOS software for the Catalyst 4006 switch with Supervisor Engine III.

Release 12.1(11b)EW provides these features:

- Multiple VLAN access port (only for data and voice VLANs)
- Inline power management for Cisco IP phones and Aironet 350 Wireless Access Points on the WS-X4148-RJ45V module.
- Power redundancy
- Multicast flooding suppression for STP changes
- IGMP filtering

New Hardware Features in Release 12.1(8a)EW

Release 12.1(8a)EW provides initial support of the Cisco IOS software for the Catalyst 4006 switch with Supervisor Engine III and the following modules:

- WS-X4124-FX-MT—24-port 100BASE-FX Fast Ethernet switching module

- WS-X4148-FX-MT—48-port 100BASE-FX Fast Ethernet switching module
- WS-X4148-RJ—48-port 10/100 Fast Ethernet RJ-45 switching module
- WS-X4148-RJ21—48-port 10/100-Mbps Fast Ethernet RJ-21 (telco connector) switching module
- WS-X4148-RJ45V—48-port inline power 10/100BASE-TX switching module: data traffic only (inline power not supported in Cisco IOS Release 12.1(8a)EW)
- WS-X4232-GB-RJ—32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet switching module
- WS-X4232-RJ-XX—32-port 10/100 Fast Ethernet RJ-45 modular uplink switching module
- WS-X4306-GB—6-port 1000BASE-X (GBIC) Gigabit Ethernet switching module
- WS-X4418-GB—18-port 1000BASE-X (GBIC) Gigabit Ethernet switching module
- WS-X4412-2GB-T—12-port 1000BASE-T Gigabit Ethernet and 2-GBIC ports switching module
- WS-X4424-GB-RJ45—24-port 10/100/1000BASE-T Gigabit Ethernet switching module
- WS-X4448-GB-LX—48-port 1000BASE-LX Gigabit Ethernet Fiber Optic interface switching module
- WS-X4448-GB-RJ45—48-port 10/100/1000BASE-T Gigabit Ethernet switching module

New Software Features in Release 12.1(8a)EW

Release 12.1(8a)EW provides initial support of the Cisco IOS software for the Catalyst 4006 switch with Supervisor Engine III.

Release 12.1(8a)EW provides these features:

- The Layer 2 features are as follows:

  Note The following chapter references are for the *Software Configuration Guide for the Catalyst 4006 Switch with Supervisor Engine III.*

  - Layer 2 switch ports and VLAN trunks with the Dynamic Trunking Protocol (DTP) (refer to the “Configuring Layer 2 Ethernet Interfaces” chapter)
  - VLANs (refer to the “Understanding and Configuring VLANs” chapter)
  - Private VLANs (refer to the “Understanding and Configuring Private VLANs” chapter)
  - VLAN Trunk Protocol (VTP) and VTP domains (refer to the “Understanding and Configuring VTP” chapter)
  - Spanning Tree Protocol (refer to the “Understanding and Configuring STP” chapter)
  - Spanning tree PortFast, UplinkFast, and BackboneFast (refer to the “Configuring STP Features” chapter)
  - IGMP snooping (refer to the “Understanding and Configuring IGMP Snooping” chapter)
- Cisco Express Forwarding for IP unicast traffic (refer to the “Configuring CEF” chapter)
- Standard Domain Naming System (DNS) support (refer to the Cisco IOS *Network Protocols Configuration Guide*, Part 1, and the Cisco IOS *Network Protocols Command Reference*, Part 1)
- Dynamic Host Configuration Protocol (DHCP); (refer to Cisco IOS *IP and IP Routing Configuration Guide*, Release 12.1, “Configuring DHCP”)

- Bootstrap Protocol (BOOTP) relay (refer to the Cisco IOS *Network Protocols Configuration Guide*, Part 1, and the Cisco IOS *Network Protocols Command Reference*, Part 1)
- Cisco Discovery Protocol (CDP); (refer to the "Understanding and Configuring CDP" chapter)
- Standard IP access control lists (ACLs) at wire rate (refer to the "Configuring Network Security" chapter)
- The Layer 3 features are as follows:
  - Layer 3 routing protocols (refer to the Cisco IOS *Network Protocols Configuration Guides*, Parts 1 and 2, and the Cisco IOS *Network Protocols Command Reference*, Parts 1 and 2):

    Static IP routing
    IP routing protocols
    IP multicast routing protocols
  - Layer-3 related protocols (refer to the Cisco IOS Release 12.1 *Network Protocols Configuration Guides*, Parts 1 and 2, and the Cisco IOS Release 12.1 *Network Protocols Command Reference*, Parts 1 and 2):

    Internet Group Management Protocol (IGMP) v1 and v2
    Cisco Group Membership Protocol (CGMP) server support
    Full Internet Control Message Protocol (ICMP) support
    ICMP Router Discovery Protocol (IRDP)
    Multicast Source Discovery Protocol (MSDP)
    Multicast Border Gateway Protocol (MBGP)
- Multiple-Hot Standby Routing Protocol (M-HSRP; refer to "Hot Standby Router Protocol" in the Cisco IOS *Network Protocols Configuration Guide*, Part 1, and the Cisco IOS *Network Protocols Command Reference*, Part 1)
- Access control using several supported authentication methods (refer to the "Configuring the Switch for the First Time" chapter)
- Switched Port Analyzer (SPAN); (refer to the "Understanding and Configuring SPAN" chapter)
- Quality of Service (QoS); (refer to the "Understanding and Configuring QoS" chapter)

Upgrading the System Software

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

Note You must upgrade to ROMMON Release 12.2(44r)SG5 to run Cisco IOS Release 12.2(54)SG on the Supervisor Engine 6-E and Supervisor Engine 6L-E.

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

Table 1 Supervisor Engine and Minimum Cisco IOS Release

Supervisor Engine	Minimum Cisco IOS Release
IV	12.1(12c)EW or 12.1(14)E
II-Plus	12.1(19)EW
II-Plus-10GE	12.2(25)SG
V	12.2(18)EW
II-Plus-TS	12.2(20)EWA
V-10GE	12.2(25)EW
ME-X4924-10GE	12.2(31)SGA
6-E	12.2(40)SG
6L-E	12.2(52)XO

Table 2 Supervisor Engine and Recommended ROMMON Release

Supervisor Engine	Minimum ROMMON Release
IV	12.1(12r)EW
II-Plus	12.1(19r)EW
II-Plus-10GE	12.2(25r)SG
V	12.1(20r)EW1
II-Plus-TS	12.2(20r)EW
V-10GE	12.2(25r)EW
ME-X4924-10GE	12.2(25r)EW
6-E	12.2(44r)SG5
6L-E	12.2(44r)SG5

Table 3 ROMMON Release and Promupgrade Programs

ROMMON Release	Promupgrade Program
12.1(11br)EW	cat4000-sup3-promupgrade-121_11br_EW
12.1(12r)EW	cat4000-sup3-promupgrade-121_12r_ew
12.1(19r)EW	cat4000-ios-promupgrade-121_19r_EW
12.1(20r)EW1	cat4000-ios-promupgrade-121_20r_EW1
12.1(20r)EW2	cat4000-ios-promupgrade-121_20r_EW2
12.2(20r)EW	cat4000-ios-promupgrade-122_20r_EW
12.2(20r)EW1	cat4000-ios-promupgrade-122_20r_EW1
12.2(31r)SG3	cat4500-ios-promupgrade-122_31r_SG3
12.2(31r)SGA1	cat4500-ios-promupgrade-122_31r_SGA1
12.2(31r)SGA	cat4500-e-ios-promupgrade-122_31r_SGA3
12.2(40r)SG	cat4500-e-ios-promupgrade-122_40r_SG

Table 3 ROMMON Release and Promupgrade Programs

ROMMON Release	Promupgrade Program
12.2(44r)SG1	cat4500-e-ios-promupgrade-122_44r_SG1
12.2(44r)SG5	cat4500-e-ios-promupgrade-122_44r_SG5

The following sections describe how to upgrade your switch software:

- Guidelines for Upgrading the ROMMON, page 17
- Upgrading the Supervisor Engine ROMMON from the Console, page 17
- Upgrading the Supervisor Engine ROMMON Remotely Using Telnet, page 20
- Upgrading the Cisco IOS Software, page 25

Guidelines for Upgrading the ROMMON

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

Upgrading the Supervisor Engine ROMMON from the Console

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

Note The examples in this section use the programmable read-only memory (PROM) upgrade version 12.1(20r)EW1 and Cisco IOS Release 12.1(20)EW1. For other releases, replace the ROMMON release and Cisco IOS software release with the appropriate releases and filenames.

Follow this procedure to upgrade your supervisor engine ROMMON:

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

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

Step 2 Download the cat4000-ios-promupgrade-121_20r_EW1 program from Cisco.com, and place it on a TFTP server in a directory that is accessible from the switch that is upgraded.

The cat4000-ios-promupgrade-121_20r_EW1 programs are available on Cisco.com at the same location from which you download Catalyst 4000 system images.

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

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

Step 4 Download the cat4000-ios-promupgrade-121_20r_EW1 program into Flash memory using the **copy tftp** command.

The following example shows how to download the PROM upgrade image cat4000-ios-promupgrade-121_20r_EW1 from the remote host 172.20.58.78 to bootflash:

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4000-ios-promupgrade-121_20r_EW1]?
Destination filename [cat4000-ios-promupgrade-121_20r_EW1]?
Accessing tftp://172.20.58.78/cat4000-ios-promupgrade-121_20r_EW1...
Loading cat4000-ios-promupgrade-121_20r_EW1 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
[OK - 455620 bytes]

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

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

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

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

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



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

 Rom Monitor Program Version 12.1(12r)EW


.
.(output truncated)
.

 Established physical link 100MB Half Duplex
 Network layer connectivity may take a few seconds
rommon 1 >
```

Step 6 Run the PROM upgrade program by entering this command:
boot bootflash:cat4000-ios-promupgrade-121_20r_EW1

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

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

```
rommon 2 > boot bootflash:cat4000-ios-promupgrade-121_20r_EW1

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

 Image size = 314.236 KBytes

 Maximum allowed size = 511.75 KBytes


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

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

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

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

 Success! The prom has been upgraded successfully.
 System will reset itself and reboot in about 15
```

Step 7 Boot the Cisco IOS software image, and enter the **show version** command to verify that ROMMON has been upgraded to 12.1(20r)EW1.

Step 8 Use the **delete** command to delete the PROM upgrade program from bootflash and the **squeeze** command to reclaim unused space.

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

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

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

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

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

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4500 L3 Switch Software (cat4500-I9S-M), Version 12.1(20)EW, E
ARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 22-Oct-03 23:42 by kellmill
Image text-base: 0x00000000, data-base: 0x00F56DDC
```

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

Switch uptime is 0 day, 0 hour, 5 minutes
System returned to ROM by reload
System image file is "bootflash:cat4500-i9s-mz.121-20.EW1"

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

Configuration register is 0x2102

Switch#
```

The ROMMON has now been upgraded.

See the "Upgrading the Cisco IOS Software" section on page 25 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Supervisor Engine ROMMON Remotely Using Telnet

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

Follow this procedure to upgrade your supervisor engine ROMMON to Release 12.1(20r)EW1. This procedure can be used when console access is not available and when the ROMMON upgrade must be performed remotely.

Note In the following section, use the PROM upgrade version cat4000-ios-promupgrade-121_20r_EW1.

Step 1 Establish a Telnet session to the supervisor engine.

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

Step 2 Download the cat4000-ios-promupgrade-121_20r_EW1 program from Cisco.com, and place it on a TFTP server in a directory that is accessible from the switch to be upgraded.

The cat4000-ios-promupgrade-121_20r_EW1 programs are available on Cisco.com at the same location from which you download Catalyst 4500 system images.

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

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

Step 4 Download the cat4000-ios-promupgrade-121_20r_EW1 program into Flash memory using the **copy tftp** command.

The following example shows how to download the PROM upgrade image cat4000-ios-promupgrade-121_20r_EW1 from the remote host 172.20.58.78 to bootflash:

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4000-ios-promupgrade-121_20r_EW1]?
Destination filename [cat4000-ios-promupgrade-121_20r_EW1]?
Accessing tftp://172.20.58.78/cat4000-ios-promupgrade-121_20r_EW1...
Loading cat4000-ios-promupgrade-121_20r_EW1 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
[OK - 455620 bytes]

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

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

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

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

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

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

Use the config-register command to autoboot using image(s) specified by the BOOT variable.
Configure the BOOT variable to upgrade the ROMMON and then autoboot the IOS image after
the ROMMON upgrade is complete. In this example, we are upgrading the ROMMON to version
12.1(20r)EW1. After the ROMMON upgrade is complete, the supervisor engine will boot Cisco
IOS software Release 12.1(20)EW1.

config-register to 0x0102.

Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch(config)# boot system flash bootflash:cat4000-i9s-mz.121-20.EW1
Switch(config)# config-register 0x0102
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

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

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

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

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

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

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

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




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

 Rom Monitor Program Version 12.1(12r)EW

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

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


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


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


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

 Current BOOT file is --- bootflash:cat4000-ios-promupgrade-121_20r_EW1
 **********************************************************
 *                                                        *
 * Rom Monitor Upgrade Utility For  WS-X4515 System       *
 * This upgrades flash Rom Monitor image to the latest    *
 *                                                        *
 * Copyright (c) 2002, 2003 by Cisco Systems, Inc.        *
 * All rights reserved.                                   *
 *                                                        *
 **********************************************************

 Image size = 314.236 KBytes

 Maximum allowed size = 511.75 KBytes


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

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

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

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

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


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

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

Rommon reg: 0x56000380

Running IOS...

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

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

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

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

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

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

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

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

Configuration register is 0x0102

Switch#
```

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

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

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

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

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

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

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

The ROMMON has now been upgraded.

See the "Upgrading the Cisco IOS Software" section on page 25 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Cisco IOS Software

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

Before you proceed, observe the following rules for hostname:

- Do not expect case to be preserved

  Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, Choosing a Name for Your Computer.

- Must start with a letter and end with a letter or digit.
- Interior characters can only be letters, digits, and hyphens; periods and underscores not allowed.
- Names must be 63 characters or fewer; hostname of fewer than 10 characters is recommended.
- On most systems, a field of 30 characters is used for the host name and the prompt in the CLI. Longer configuration mode prompts may be truncated.

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

Step 1 Download Cisco IOS Release 12.1(20)EW from Cisco.com, and place the image on a TFTP server in a directory that is accessible from the supervisor engine that is upgraded.

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

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

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

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

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

```
[OK - 6923388/13846528 bytes]

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

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

The following example shows how to clear the BOOT variable:

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

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

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

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

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

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

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

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

Caution No intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the upgrade process by performing a reset, power cycle, or OIR of the supervisor, for at least five minutes.

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

```
Switch# reload
Rommon reg: 0x2B004180

Upgrading FPGA...

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

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

 Image size = 483.944 KBytes

 Maximum allowed size = 1023.75 KBytes


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

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

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

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

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




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

 Rom Monitor Program Version 12.1(12r)EW

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


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

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


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

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

Limitations and Restrictions

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

All Supervisor Engines

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

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

  The outputs of certain commands, such as **show ip route** and **show access-lists**, contain non-deterministic text. While the output is easily understood, the output text does not contain strings that are consistently output. A general purpose specification file entry is unable to parse all possible output.

  Workaround (1):

  While a general purpose specification file entry may not be possible, a specification file entry might be created that returns the desired text by searching for text that is guaranteed to be in the output. If a string is guaranteed to be in the output, it can be used for parsing.

  For example, the output of the show ip access-lists SecWiz_Gi3_17_out_ip command is this:

```
Extended IP access list SecWiz_Gi3_17_out_ip
    10 deny ip 76.0.0.0 0.255.255.255 host 65.65.66.67
    20 deny ip 76.0.0.0 0.255.255.255 host 44.45.46.47
    30 permit ip 76.0.0.0 0.255.255.255 host 55.56.57.57
```

  The first line is easily parsed because access list is guaranteed to be in the output:

```
    <Property name="access list" alias="Name" distance="1.0" length="-1" type="String"
/>
```

The remaining lines all contain the term host. As a result, the specification file may report the desired values by specifying that string. For example, this line

```
    <Property name="host" alias="rule" distance="s.1" length="1" type="String" />
```

will produce the following for the first and second rules

```
    <rule>
        deny
    </rule>
```

and the following for the third statement

```
    <rule>
        permit
    <rule>
```

Workaround (2):

Request the output of the **show running-config** command using NETCONF and parse that output for the desired strings. This is useful when the desired lines contain nothing in common. For example, the rules in this access list do not contain a common string and the order (three permits, then a deny, then another permit), prevent the spec file entry from using permit as a search string, as in the following example:

```
    Extended MAC access list MACCOY
        permit 0000.0000.ffef ffff.ffff.0000 0000.00af.bcef ffff.ff00.0000 appletalk
        permit any host 65de.edfe.fefe xns-idp
        permit any any protocol-family rarp-non-ipv4
        deny   host 005e.1e5d.9f7d host 3399.e3e1.ff2c dec-spanning
        permit any any
```

The XML output of **show running-config** command includes the following, which can then be parsed programmatically, as desired:

```
<mac><access-list><extended><ACLName>MACCOY</ACLName></extended></access-list></mac>
    <X-Interface> permit 0000.0000.ffef ffff.ffff.0000 0000.00af.bcef ffff.ff00.0000
appletalk</X-Interface>
    <X-Interface> permit any host 65de.edfe.fefe xns-idp</X-Interface>
    <X-Interface> permit any any protocol-family rarp-non-ipv4</X-Interface>
    <X-Interface> deny   host 005e.1e5d.9f7d host 3399.e3e1.ff2c
dec-spanning</X-Interface>
    <X-Interface> permit any any</X-Interface>
```

- Although the Catalyst 4500 series switch still supports legacy 802.1X commands used in Cisco IOS Release 12.2(46)SG and earlier releases (that is, they are accepted on the CLI), they do not display in the CLI help menu.
- Current IOS software cannot support filenames exceeding 64 characters.
- All software releases support a maximum of 32,768 IGMP snooping group entries.

For Supervisor Engines II+Plus through V-10GE

- For the IP Unnumbered feature, the following are not supported:
  - Dynamic routing protocols
  - HSRP/VRRP

    - Static ARP
    - Unnumbered interface and numbered interface in different VRFs
- For WCCP version 2, the following are not supported:
    - GRE encapsulation forwarding method
    - Hash bucket based assignment method
    - Redirection on an egress interface (redirection out)
    - Redirect-list ACL
- For IPX software routing, the following are not supported:
    - NHRP (Next Hop Resolution Protocol)
    - NLSP
    - Jumbo Frames
- For AppleTalk software routing, the following are not supported:
    - AURP
    - AppleTalk Control Protocol for PPP
    - Jumbo Frames
    - EIGRP
- For the NetFlow feature, the following limitations apply:
    - NetFlow will not account for control packets, packets that encountered link-level errors, and ARP/RARP packets.
    - The software cache for NetFlow is fixed, users cannot change the size.
    - The statistical distribution row that displays the distribution across various packet sizes is not available.
- For the PBR feature, the following limitations apply:
    - Packet length-based matching policies are not supported.
    - IP Precedence, TOS and Qos groups are fixed.
    - ACL/Route-map statistics are not updated.
- IGRP is not supported (use EIGRP instead).
- The MAC address table is cleared when you switch between supervisor engines if either the 802.1s or 802.1w Spanning Tree Protocol is configured. To minimize address clearing and subsequent packet flooding, configure the edge ports as **spanning-tree portfast** and the link type as **spanning-tree link-type point-to-point**.
- While running NSF and IS-IS IETF mode, if you enter the **issu runversion** command within 5 minutes of entering the **issu loadversion** command, packet loss may occur during an ISSU upgrade.

  Workaround: Configure the NSF interval timer to 0 minutes, or delay entering the **issu runversion** command until the NSF interval timer expires and NSF restarts.
- Routes may not be properly redistributed from one routing protocol to another when NSF is enabled on the switch. The success of the redistribution depends on the order in which the routing protocols converge after an NSF switchover.

  Workaround: None.

- IP classful routing is not supported; do not use the **no ip classless** command; it will have no effect because only classless routing is supported. The **ip classless** command is not supported because classless routing is enabled by default.
- The Catalyst 4510R switch does not support Supervisor Engines II-Plus, III, IV, and II-Plus-10GE. Installing an unsupported supervisor engine causes unpredictable hardware behavior that cannot be controlled by the software. Using an unsupported supervisor engine in a redundant slot might cause a supported supervisor engine in the other slot to malfunction.
- Supervisor Engine II-Plus cannot read a CompactFlash card formatted by Supervisor Engine III or Supervisor Engine IV in a prior release.
- Catalyst 4500 supervisor engines will not be properly initialized if the VLAN configuration in the startup file does not match the information stored in the VLAN database file. This situation might occur if a backup configuration file was used.
- A Layer 2 LACP channel cannot be configured with the spanning tree PortFast feature.
- Netbooting using a boot loader image is not supported. See the "There are no resolved caveats in software release 12.1(8a)EW." section on page 172 for alternatives.
- You cannot downgrade to Cisco IOS Release 12.1(8a)EW1 after running Release 12.1(13)EW (or higher). If you need to downgrade, contact your TAC representative for further instructions, and mention caveat CSCdz59058.
- Observe the following standard Cisco IOS software behavior when deploying redundant supervisor engines in a Catalyst 4507R chassis: While the startup configuration file is being parsed, the configuration file is not applied to hardware that does not exist.

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

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

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

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

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

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

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

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

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

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

- You can run .1q-in-.1q packet passthrough with a Supervisor Engine III and a Supervisor Engine IV, but you can run only .1q-in-.1q encapsulation with a Supervisor Engine II+10GE, Supervisor Engine V, and Supervisor Engine V-10GE.
- For PVST and Catalyst 4500 E-Series switch VLAN, Cisco IOS Release 12.1(13)EW supports a maximum of 3000 spanning tree port instances. If you want to use more instances, use MST rather than PVST.
- Only ports 1 and 2 on the WS-X4418-GB module and ports 13 and 14 on the WS-X4412-2GB-T module can be set as ISL trunks.
- If an original packet is dropped due to transmit queue shaping or sharing configurations, a SPAN packet copy can still be transmitted on the SPAN port.
- For all software releases, do not use over 100,000 routes.
- Use the **no ip unreachables** command on all interfaces with ACLs configured for performance reasons.
- Layer 3 path load-balancing metrics are not supported in Cisco IOS Releases 12.1(8a)EW, 12.1(11b)EW, 12.1(12c)EW, 12.1(13)EW, 12.1(19)EW, and 12.1(20)EW. (CSCdv10578)
- The threshold for the Dynamic ARP Inspection err-disable function is set to 15 ARP packets per second per interface. You should adjust this threshold depending on the network configuration. The CPU should not receive DHCP packets at a sustained rate greater than 1000 pps.
- A limited number of ACL bindings are dynamically installed by the IP source guard feature on a Catalyst 4500 series switch Supervisor Engine II-Plus. To take full advantage of the IP source guard feature, you should use Supervisor Engine IV.
- If you first configure an IP address or IPv6 address on a Layer 3 port, then change the Layer 3 port to a Layer 2 port with the **switchport** command, and finally change it back to a Layer 3 port, the original IP/IPv6 address is lost.
- By default, IPv6 is not enabled. To route IPv6, you must enter the **IPv6 unicast-routing** command. If you plan to use IPv6 multicast routing, use the **IPv6 multicast-routing** command.
- By default, CEF is not enabled for IPv6 (after IPv6 unicast routing is enabled). To prevent IPv6 traffic from being process-switched, use the **IPv6 cef** command.
- Multicast sources in community VLANs are not supported.
- Two-way community VLANs are not supported.
- Voice VLANs are not supported on community VLAN host interfaces.
- Private VLAN trunks do not carry community VLANs.
- When you use private VLANs on the WS-4516 module, old ARP entries will not tim eout of the ARP cache if you do not manually clear the entry. This event has no affect on production.
- Compact flash formatted in Cisco IOS Release 12.2(20)EW should be reformatted in Release 12.2(25)EW on both Supervisor Engine V-10GE and non-Supervisor V-10GE systems. Compact flash formatted on any other release does not need to be reformatted on non-Supervisor Engine V-10GE systems.
- In a redundant system, do not remove and reinsert the standby supervisor engine while the active supervisor engine is booting up. Doing so may cause a failure in the online diagnostics test.

  Workaround: Remove and reinsert the standby supervisor engine after the active supervisor engine boots. (CSCsa66509)

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

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

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

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

  If this message appears, verify that the switch is connected to the ACS. You should also ensure that the switch has been properly configured as an AAA client on the ACS.
- The **bgp shutdown** command is not supported in BGP router configuration mode. Entering this command might produce unexpected results.
- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

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

  Workarounds:

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

  2. Configure the media converter to autonegotiate the speed and duplex instead of running them at 100 Mbps and full duplex. (CSCee62109)

- IPSG for static hosts supports the same port mode as IPSG except that it does not support trunk port:
  - It supports Layer 2 access port and PVLAN host port (isolated or community port).
  - It does not support trunk port, Layer 3 port, or EtherChannel.
- IPSG for static hosts should not be used on uplink ports.
- Selective DBL is only supported for non-tagged or single-tagged IP packets. To achieve Selective DBL-like functionality with a non-IP packet (like Q-in-Q and IPX), apply an input policy map that matches CoS values and specifies DBL in the class map.
- For Selective DBL, if the topology involves Layer 2 Q in Q tunneling, the match cos policy map will apply to the incoming port.
- If a set of DSCP values are already configured (for example, 0-30, 0-63), specifying a subset of these DSCP values with the **qos dbl dscp-based 0-7** command will not remove the unwanted DSCP values of 8 through 63. You must use the **no** form of the command to remove the extraneous values. In this case, the **no qos dbl dscp-based 8-63** command will leave 0-7 selected.
- When you use Port Security with Multi Domain Authentication (MDA) on an interface:
  - Allow for at least three MAC addresses to access the switch: two for the phone (the MAC address of a phone gets registered to the Data domain and Voice domain), and one for the PC.
  - Ensure that the data and voice VLAN IDs differ.
- For IP Port Security (IPSG) for static hosts, the following apply:
  - As IPSG learns the static hosts on each interface, the switch CPU may achieve 100 percent if there are a large number of hosts to learn. CPU usage will drop after the hosts are learned.
  - IPSG violations for static hosts are printed as they occur. If multiple violations occur simultaneously on different interfaces, the CLI displays the last violation. For example, if IPSG is configured for 10 ports and violations exist on ports 3, 6, and 9, the violation messages are printed only for port 9.
  - Inactive host bindings will appear in the device tracking table when either a VLAN is associated with another port or a port is removed from a VLAN. So, as hosts are moved across subnets, the hosts appear in the device tracking table as Inactive.
  - Autostate SVI does not work on EtherChannel.
- With the resolution of CSCsg08775, a GARP ACL entry is no longer part of the Static CAM area. However, a system-defined GARP class in Control Plane Policing (CPP) still exists.

- Certain configurations on the Catalyst 4507R and Catalyst 4510R chassis exceed the available maximum data power. These configurations include a combination of the follow PIDs:
  - Seven-slot configuration
  - Chassis WS-C4507R-E, WS-C4510R-E
  - Dual supervisor WS-X45-Sup6-E
  - One or more of the models WS-X4448-GB-RJ45 or WS-X4148-FX-MT

  To maximize the 10/100/1000 port density of 7- and 10-slot chassis when using redundant Supervisor Engine 6-E, install WS-X4548-GB-RJ45 instead of WS-X4448-GB-RJ45 line cards. If you require WS-X4448-GB-RJ45 line cards, two options are available:
  - Option 1

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

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

  To maximize the 100-BASE-FX port density of 7 and 10 slot chassis when using Supervisor Engine 6-E install WS-4248-FE-SFP line cards with FX optics instead of WS-X4148-FX-MT line cards. If WS-X4148-FX-MT line cards are required, two options are available:
  - Option 1

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

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

  ```
  % Hardware MTU table exhausted
  ```

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

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

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

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

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

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

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

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

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

- The Catalyst 4510R switch does not support Supervisor Engines 6L-E. Installing an unsupported supervisor engine causes unpredictable hardware behavior that cannot be controlled by the software. Using an unsupported supervisor engine in a redundant slot might cause a supported supervisor engine in the other slot to malfunction.
- The MAC address table is cleared while you switch between supervisor engines if either the 802.1s or 802.1w Spanning Tree Protocol is configured. To minimize address clearing and subsequent packet flooding, configure the edge ports as **spanning-tree portfast** and the link type as **spanning-tree link-type point-to-point**.
- IP classful routing is not supported; do not use the **no ip classless** command; it will have no effect, because only classless routing is supported. The command **ip classless** is not supported because classless routing is enabled by default.
- A Layer 2 LACP channel cannot be configured with the spanning tree PortFast feature.
- Netbooting using a boot loader image is not supported. See the "There are no resolved caveats in software release 12.1(8a)EW." section on page 172 for alternatives.
- When you deploy redundant supervisors in a Catalyst 4507R, for hardware that does not exist while the startup configuration file is being parsed, the configuration file for the hardware is not applied.

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

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

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

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

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

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

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

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

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

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

  Workaround: Ensure that the MTUs match.

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

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

  - Supervisor Engine 6-E uses the FAT file system for compact flash (slot0). If a compact flash is not formatted in FAT file system (such as compact flash on a supervisor engine other than 6-E), the switch does not recognize it.

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

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

  PoE switching modules:

  - WS-X4148-RJ45V
  - WS-X4224-RJ45V
  - WS-X4248-RJ45V
  - WS-X4248-RJ21V
  - WS-X4524-GB-RJ45V
  - WS-X4548-GB-RJ45V
  - WS-X4648-RJ45V-E
  - WS-X4648-RJ45V+E
  - WS-X4548-GB-RJ45V+

  PoE enabled power supplies:

  - PWR-C45-1300ACV
  - PWR-C45-1400DC
  - PWR-C4K-2800AC
  - PWR-C45-1400AC
  - PWR-C45-1300ACV
  - PWR-C45-6000ACV
- If a Catalyst 4500 series switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

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

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

- For IP Port Security (IPSG) for static hosts, the following apply:
  - As IPSG learns the static hosts on each interface, the switch CPU may achieve 100 percent if there are a large number of hosts to learn. The CPU usage will drop after the hosts are learned.
  - IPSG violations for static hosts are printed as they occur. If multiple violations occur simultaneously on different interfaces, the CLI displays the last violation. For example, if IPSG is configured for 10 ports and violations exist on ports 3,6, and 9, the violation messages are printed only for port 9.
  - Inactive host bindings will appear in the device tracking table when either a VLAN is associated with another port or a port is removed from a VLAN. So, as hosts are moved across subnets, the hosts appear in the device tracking table as inactive.
  - Autostate SVI does not work on EtherChannel.
- When IPv6 is enabled on an interface with any CLI, you might see the following message:

```
% Hardware MTU table exhausted
```

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

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

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

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

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

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

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

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

- uRPF supports up to four paths. If a packet arrives at one of the valid VLANs that is not programmed as one of the RPF VLAN in hardware, it is dropped. If traffic may arrive from any other interfaces without RPF configured, it can be switched.
- Input and output ACLs cannot override or filter traffic received on an uRPF interface.
- No CLI command exists to reflect uRPF drop packets during hardware switching. The **sh ip traffic** and **show cef int** commands do not reflect uRPF drops.
- IPv6 ACL is not supported on a switchport. IPv6 packets cannot be filtered on switchports using any of the known methods: PACL, VACL, or MACLs.

- Class-map match statements using **match ip prec | dscp** match only IPv4 packets, whereas matches performed with **match prec | dscp** match both IPv4 and IPv6 packets.
- IPv6 QoS hardware switching is disabled if the policy-map contains IPv6 ACL and match CoS in the same class-map with the IPv6 access-list has any mask within the range /81 and /127. This situation causes forwarding packets to software, which efficiently disables the QoS.
- When the following data-only Catalyst 4500 linecards are used in a Catalyst 4507R-E or 4510R-E chassis with Supervisor Engine 6-Es, the capacity of the power supply may be exceeded:
  - WS-X4148-FX-MT Cisco Catalyst 4500 Fast Ethernet Switching Module, 48-port 100BASE-FX (MT-RJ)
  - WS-X4448-GB-RJ45 Cisco Catalyst 4500 48-port 10/100/1000 Module (RJ-45)

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

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

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

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

- Supervisor Engine 6-E *only* supports Catalyst 4500 Series linecards in slots 8-10.
- If you remove a line card from a redundant switch and initiate an SSO switch-over, then reinsert the line card, all interfaces are shutdown. The remaining configuration on the original line card is preserved.

  This situation only occurs if a switch reached SSO before you removed the line card.
- On Supervisor Engine 6-E, upstream ports support flow control auto negotiation in 1G mode only, and flow control is forced in 10G mode. If the interface is configured to auto-negotiate the flow control, and the interface is operating in 10G mode, the system forces flow control to ON and does not auto-negotiate.
- Supervisor Engine 6-E supports fast UDLD on a maximum of 32 ports.

Caveats

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

Note All caveats in Release 12.4 also apply to the corresponding 12.1 E releases. Refer to the *Caveats for Cisco IOS Release 12.4* publication at the following URL:

http://www.cisco.com/en/US/docs/ios/12_4/release/notes/124MCAVS.html

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

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

Open Caveats in Cisco IOS Release 12.2(25)EWA14

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA14:

- While configuring Smartport macros via HTTP interactively, a switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser *command* area as if you were entering the commands through the CLI. (CSCei76082)

- A switch upgrading to Cisco IOS Releases 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This caveat is cosmetic only; it does not impact the operation of the switch.

  Workaround: Power-cycle the switch. (CSCsg00796)

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

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA14

This section lists the resolved caveat in Cisco IOS Release 12.2(25)EWA14:

- On a Catalyst 4500 series switch with either dual 4200W AC power supplies with one or both 220V connections, or a single 4200W AC power supply with two 220V connections, a power supply firmware glitch temporarily resets the status bits. It causes Catalyst 4500 IOS software to receive the false input voltage values (from 220V to 110V) and trigger the normal recovery routine.

  You will see one or both of the following error messages:

  ```
  *Mar 5 11:16:33.663 UTC: %C4K_CHASSIS-3-MIXINVOLTAGEDETECTED: Power supplies in the
  chassis are receiving different voltage inputs
  *Mar 5 11:16:33.663 UTC: %C4K_CHASSIS-3-MIXINPOWERDETECTED: Power supplies in the
  chassis are of different types (AC/DC) or wattage
  ```

You may also see the following message:

```
%ILPOWER-5-ILPOWER_POWER_DENY: Interface Gi2/33: inline power denied
On ports with POE devices connected.
```

This glitch temporarily shuts down the affected power supply and causes a loss of power supply redundancy. Power for the data and chassis is decremented and might cause the linecard(s) to shut down. Power for PoE also will decrement, and it could cause PDs to shut down and reset.

Note the following:

- Only units with serial numbers starting from with AZS12200001 and higher *do not* experience this defect.
- If both power supplies have 110V inputs, they are *not* affected.
  The output current will be lower with both 110V input connections, see
  Power Supply Calculator on cisco.com at the URL http://tools.cisco.com/cpc/launch.jsp.

Workaround: None. (CSCso67729)

- A group of 4 ports on a PoE linecard might *not* recognize the IEEE phone device and might *not* provide inline power. The same device(s) may work in other ports on the same module; it may work with other ports of similar linecards in other slots on the same chassis.

  The group(s) of ports on which the PoE devices do not power up may differ in every instance.

  The problem has been observed with the following hardware combinations:

  - 4500 chassis, WS-X4013+=, WS-X4548-GB-RJ45V= (hw rev 4.0 & 4.1), 12.2(40)SG
  - 4500-E chassis WS-C45-Sup6-E, WS-X4548-GB-RJ45V= (hw rev 4.0 & 4.1), 12.2(40)SG

Note Cisco IP Phone is not affected as it can be detected via CDP.

Workaround: None. (CSCso29149)

- A Catalyst 4500 switch may experience a reload if you perform two or more
  “write memory's via CLI” on the switch.

  This occurs with Cisco IOS Releases 12.2(25)EWA13 and earlier releases, 12.2(31)SGA6 and earlier releases, and 12.2(4x)SG releases.

  Workaround: Restrict *vty access* to one session and upgrade to Cisco IOS Release 12.2(25)EWA14 or 12.2(31)SGA7. (CSCso86459)

- On a Catalyst 4500 Supervisor Engine running Cisco IOS Releases 12.2(25)EWA13, or
  12.2(31)SGA4 through 12.2(31)SGA6, you might receive the message
  "NVRAM Verification Failed" and the running config might not be saved to the NVRAM.

  Workaround: Upgrade to Cisco IOS Release 12.2(25)EWA14 or 12.2(31)SGA7. (CSCsq27434)

Open Caveats in Cisco IOS Release 12.2(25)EWA13

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA13:

- While configuring Smartport macros via HTTP interactively, a switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser *command* area as if you were entering the commands through the CLI. (CSCei76082)

- A switch upgrading to Cisco IOS Releases 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

```
Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
```

This caveat is cosmetic only; it does not impact the operation of the switch.

Workaround: Power-cycle the switch. (CSCsg00796)

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

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA13

This section lists the resolved caveat in Cisco IOS Release 12.2(25)EWA13:

- After auto-QoS is enabled on a switch, data traffic may be dropped when Dynamic Buffer Leaking (DBL) is enabled.

  While this problem occurs, traffic drops appear under the Dbl-Drop-Queue counter on the output of the **show interface <mod/port> counter detail** command.

  Workaround: Disable DBL globally by configuring the **no qos dbl** command. (CSCsk07525)

- When MSDP and OSPF are configured, the MSDP timer is set to 1, and you issue the **no ip routing** command, the switch reloads because of memory corruption in one of the pointerrs used by MSDP.

  The caveat does not occur if the MSDP timer is greater than 1.

  Workaround: Increase the MSDP timer to 5. (CSCsj61328)

Open Caveats in Cisco IOS Release 12.2(25)EWA12

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA12:

- While configuring Smartport macros via HTTP interactively, a Catalyst 4500 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- A Catalyst 4500 series switch upgrading to IOS versions 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This does not impact the operation of the Catalyst 4500 series switch, appearing to be strictly cosmetic.

  Workaround: Power-cycle the switch. (CSCsg00796)

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

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA12

This section lists the resolved caveat in Cisco IOS Release 12.2(25)EWA12:

- If a switch has a redundant supervisor, under rare conditions you will observe the following situation: You first observe the *keepalive missing* warning messages. Then, after the keepalive protocol times out, a switchover to the standby supervisor engine occurs. **4500 only**

  This happens because the active and standby supervisor engines refer to the same seed metric for calculating the EOBC collision back off timer. Consequently, the EOBC channel might get locked in infinite collisions.

  Workaround: Upgrade the software to either:

  - Cisco IOS Release 12.2(31)SGA2 and higher, or
  - Cisco IOS Release 12.2(37)SG and higher

  (CSCsh44170)

- When connecting an end device installed with Intel 82471 to a 10/100/1000BaseTX port on a Catalyst 4948 switch with both sides (the switch port and the end device) set to auto, the speed downshifts from 1000 to 100 in autonegotiate mode when the switch side reloads and the end device is *still alive* (powered on and functional).

  The problem is not observed if the third party device reloads while the switch is *still alive*.

  Workaround: Enter the **shutdown** command followed by a **no shutdow**n command on the switch port. (CSCsk54053)

- On a Cisco router that functions as an ISR configured for OSPF, shortly after OSPF adjacencies come up, the router crashes because of a bus error.

  Workaround: Either enter the **area 0** command in the OSPF VRF process or enter the **no capability transit** command in the OSPF VRF process. (CSCsi84089)

- On a Catalyst 4948 switch running Cisco IOS Release 12.2(31)SGA, after removing and reinserting the fiber cable into the SFP, the link may not come up immediately.

  Workaround: Either remove and reinsert the SFP or issue a **shutdown** command followed by the **no shutdown** command on the affected Catalyst 4948 interface. CSCsj67573

- Typically, in Cisco IOS Releases 12.2(25)EWA10, 12.2(25)EWA11, 12.2(31)SG, and 12.2(31)SGA1, the output of the **show power inline** command is unexpectedly high:

  ```
  Switch# show power inline Fast 5/3
  Available:1400(w)  Used:4294847(w)  Remaining:-4293447(w)

  Interface Admin  Oper            Power(Watts)     Device              Class
                              From PS    To Device
  --------- ------ ---------- ---------- ---------- ------------------- -----

  Fa5/3     auto   on         429496     42944.     IP Phone 7961       2
  ```

  As a result of this issue, you might observe log messages like the following:

  ```
  %C4K_IOSMODPORTMAN-4-INLINEPOWEROVERWARNING: Inline power exceeds threshold: Module
  status changed to 'Pwr Over'

  %C4K_IOSMODPORTMAN-6-INLINEPOWEROK: Inline power within limits: Module status changed
  to 'Ok'

  %C4K_IOSMODPORTMAN-6-MODULEONLINE: Module 6 (WS-X4548-GB-RJ45V S/N: JAExxxxxxxx Hw:
  3.3) is online
  ```

Workaround: Either downgrade to Cisco IOS Release 12.2(25)EWA9 or an earlier release, or upgrade to Cisco IOS Release 12.2(31)SGA2 and later releases, or Cisco IOS Release 12.2(37)SG. (CSCsj47170)

- When you add the **ip ssh ver 2** command to the configuration of the primary supervisor engine and you *fail over* to the secondary supervisor engine, the command is present in the configuration of the secondary supervisor engine. However, when you *fail back* to the primary supervisor engine, the command disappears from the configuration of the primary supervisor engine, affecting your SSH sessions.

  Workaround: None. (CSCsj51666)

Open Caveats in Cisco IOS Release 12.2(25)EWA11

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA11:

- While configuring Smartport macros via HTTP interactively, a Catalyst 4500 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- A Catalyst 4500 series switch upgrading to IOS versions 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This does not impact the operation of the Catalyst 4500 series switch, appearing to be strictly cosmetic.

  Workaround: Power-cycle the switch. (CSCsg00796)

- A Catalyst 4500 series switch running Cisco IOS Release 12.(25)EWA8 will send in dot1q tagged cdp packets when dot1x is enabled on a voice VLAN port. This might cause gigabit IP phones to send in packets that are untagged, moving the phone into the data VLAN.

  Workaround: Do either of the following:

  - Remove dot1x from the port.
  - Upgrade the IOS image to Cisco IOS 12.2(31)SGA or later.

  (CSCsg10135)

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

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- A Catalyst 4500 series switch might experience high CPU utilization due to the Cat4k Mgmt LoPri process and the K2CpuMan and K2L2 Address Table reviews (using the **show platform health** command.

  High CPU utilization does not impact the traffic switched in hardware.

  The problem is seen when a large MAC address table exists and when the switch is frequently relearning MAC addresses on multiple VLANs. Enabling the **service internal** command followed by the **debug platform log feature k2l2addresstable** command will display output similar to the following:

Note Do not enable these commands on a production switch unless instructed by Cisco TAC.

```
*Nov 13 12:56:32.066 CLT-1: K2L2AddressTableMan::newEntry index 61956 vlan 1020
address 00:D0:02:2D:38:1A
*Nov 13 12:56:34.030 CLT-1: K2L2AddressTableMan::deleteEntry index 55620 vlan 1010
address 00:D0:02:2D:38:1A
*Nov 13 12:56:34.046 CLT-1: K2L2AddressTableMan::newEntry index 55620 vlan 1010
address 00:D0:02:2D:38:1A
*Nov 13 12:56:34.062 CLT-1: K2L2AddressTableMan::deleteEntry index 61956 vlan 1020
address 00:D0:02:2D:38:1A
```

Workaround: None. (CSCsg76868)

- If a switch has a redundant supervisor, under rare conditions you will observe the following situation: You first observe the *keepalive missing* warning messages. Then, after the keepalive protocol times out, a switchover to the standby supervisor engine ocuurs. **4500 only**

  This happens because the active and standby supervisor engines refer to the same seed metric for calculating the EOBC collision back off timer. Consequently, the EOBC channel might get locked in infinite collisions.

  Workaround: Upgrade the software to either:

  - Cisco IOS Release 12.2(31)SGA2 and higher, or
  - Cisco IOS Release 12.2(37)SG and higher

  (CSCsh44170)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA11

This section lists the resolved caveat in Cisco IOS Release 12.2(25)EWA11:

- In software releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

  Workaround: None.

  This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

  Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

  A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

Open Caveats in Cisco IOS Release 12.2(25)EWA10

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA10:

- While configuring Smartport macros via HTTP interactively, a Catalyst 4500 series switch might restart unexpectedly.

Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- A Catalyst 4500 series switch upgrading to IOS versions 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This does not impact the operation of the Catalyst 4500 series switch, appearing to be strictly cosmetic.

  Workaround: Power-cycle the switch. (CSCsg00796)

- A Catalyst 4500 series switch running Cisco IOS Release 12.(25)EWA8 will send in dot1q tagged cdp packets when dot1x is enabled on a voice VLAN port. This might cause gigabit IP phones to send in packets that are untagged, moving the phone into the data VLAN.

  Workaround: Do either of the following:

  - Remove dot1x from the port.
  - Upgrade the IOS image to Cisco IOS 12.2(31)SGA or later.

  (CSCsg10135)

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

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- A Catalyst 4500 series switch might experience high CPU utilization due to the Cat4k Mgmt LoPri process and the K2CpuMan and K2L2 Address Table reviews (using the **show platform health** command.

  High CPU utilization does not impact the traffic switched in hardware.

  The problem is seen when a large MAC address table exists and when the switch is frequently relearning MAC addresses on multiple VLANs. Enabling the **service internal** command followed by the **debug platform log feature k2l2addresstable** command will display output similar to the following:

Note Do not enable these commands on a production switch unless instructed by Cisco TAC.

```
*Nov 13 12:56:32.066 CLT-1: K2L2AddressTableMan::newEntry index 61956 vlan 1020
address 00:D0:02:2D:38:1A
*Nov 13 12:56:34.030 CLT-1: K2L2AddressTableMan::deleteEntry index 55620 vlan 1010
address 00:D0:02:2D:38:1A
*Nov 13 12:56:34.046 CLT-1: K2L2AddressTableMan::newEntry index 55620 vlan 1010
address 00:D0:02:2D:38:1A
*Nov 13 12:56:34.062 CLT-1: K2L2AddressTableMan::deleteEntry index 61956 vlan 1020
address 00:D0:02:2D:38:1A
```

  Workaround: None. (CSCsg76868)

- If a switch has a redundant supervisor, under rare conditions you will observe the following situation: You first observe the *keepalive missing* warning messages. Then, after the keepalive protocol times out, a switchover to the standby supervisor engine ocuurs. **4500 only**

  This happens because the active and standby supervisor engines refer to the same seed metric for calculating the EOBC collision back off timer. Consequently, the EOBC channel might get locked in infinite collisions.

Workaround: Upgrade the software to either:

  - Cisco IOS Release 12.2(31)SGA2 and higher, or
  - Cisco IOS Release 12.2(37)SG and higher

(CSCsh44170)

- In software releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

  Workaround: None.

  This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

  Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

  A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA10

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA10:

- On PoE line cards connected to IP phones or other PoE networking devices, you might see a S2W console warning message indicating that the POE devices are either not responding to polling from the supervisor or the devices are in an an error state. When this situation exists, PoE service may not work correctly. For instance, phones will not have power or power will be removed intermittently from some ports.

  This might happen for the following reasons:

  - There is a marginal or failing component(s) on the line card (requires RMA and EFA).
  - The hardware and software states are not synchronized due to a power *glitch* or to a reset of the -48V PoE.

  This situation occurs on Cisco IOS Release 12.2(31)SGA1 or lower (except for Cisco IOS Release 12.2(25)EWA10).

Note This situation does not exist on the WS-X4148-RJ45V.

Workaround: Download an image that supports PoE Health Monitoring such as Cisco IOS Release 12.2(37)SG, 12.2(31)SGA2, or 12.2(25)EWA10. These software images have code that will monitor, detect, and attempt to correct random S2W errors. Although this code does not prevent the problem, it will positively identify the issue and and reduce recovery time.

If you experience three HealthCheck warning messages within a week, RMA the line card immediately, and request an Engineer Failure Analysis (EFA) report. Perform the following debugging steps if your IP phone or PoE device fails:

Step 1 Determine if the IP phone works using other ports on the same line card.

Step 2 Determine if the same IP phone works using another line card(s) within the switch.

Step 3 Capture **show tech-support** and **show platform chassis module** *module*.

Step 4 Reset the linecard by issuing **hw-module module** *module* **reset** or by removing and reinserting the line card. Determine if the IP phone receives power from the switch.

Step 5 Capture **show tech-support** and **show platform chassis module** *module*.

Step 6 RMA the line card if the problem persists with RMA. Ask the TAC engineer to create an EFA.

(CSCsf26804) **4500 only**

- If IGMP snooping and multicast routing are configured on a Catalyst 4500 series switch, and the switch is acting as a group querier and receives an IGMP group-specific query, the switch clears the entry from its IGMP group membership table after two seconds.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SGA2 or 12.2(25)EWA10. (CSCsh65870)

- Windows XP PCs configured for machine authentication and PEAP may not receive an updated IP address from the DHCP server based on user credentials if the PC has been machine authenticated and can ping its previously assigned default gateway.

  Workaround: Upgrade to Cisco IOS Release 12.2(25)EWA10 or 12.2(31)SGA2. (CSCsi34572)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

- For switches running IOS software prior to Release 12.2(25)EWA10, DHCP snooping syslog statistics may not be sufficient for some debugging scenarios..

  Workaround: Upgrade to Cisco IOS Release 12.2(25)EWA10. (CSCsg91116)

- Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected Cisco IOS and Cisco IOS XR devices, and may also cause a crash of the affected Cisco IOS device. Successful exploitation on an affected device running Cisco IOS XR will not cause a crash of the device itself, but may cause a crash of the IPv6 subsystem.

  Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  (CSCef77013)

- The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can cause a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  (CSCin95836)

- The server side of the Secure Copy (SCP) implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

  The Cisco IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS Secure Copy Server service are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS Secure Copy Client feature.

  (CSCsc19259)
- A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.
- A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  (CSCsi01470)

Open Caveats in Cisco IOS Release 12.2(25)EWA9

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA9:

- While configuring Smartport macros via HTTP interactively, a Catalyst 4500 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)
- A Catalyst 4500 series switch upgrading to IOS versions 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This does not impact the operation of the Catalyst 4500 series switch, appearing to be strictly cosmetic.

  Workaround: Power-cycle the switch. (CSCsg00796)
- A Catalyst 4500 series switch running Cisco IOS Release 12.(25)EWA8 will send in dot1q tagged cdp packets when dot1x is enabled on a voice VLAN port. This might cause gigabit IP phones to send in packets that are untagged, moving the phone into the data VLAN.

  Workaround: Do either of the following:

  - Remove dot1x from the port.
  - Upgrade the IOS image to Cisco IOS 12.2(31)SGA or later.

  (CSCsg10135)

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

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA9

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA9:

- When you telnet to a switch and configure the **autocommand-options nohangup** command on line vty 0 4, it will disappear After you exit. (If you look at the running configuration from the console connection, the command is not present.) This does not impact vty 5 15.

  Workaround: Open 6 telnet sessions. (CSCsg41842)

- When UDP Small Servers is enabled on an HSRP active router and it receives a UDP ECHO to the virtual ip address, the router fails to echo back by LOOPPAK.

  Workaround: None. (CSCsh13542)

- If you resume another Secure Shell (SSH) session after disconnecting an SSH session, the client console or vty will not respond until the server disconnects the session.

  Workaround: None. (CSCsd76601)

- While either initiating a Secure Shell (SSH) session from a router or copying a file to/from the router via SCP, a router may reload due to software forced crash.

  Prior to the crash, the router logs a series of %SYS-3-CPUHOG messages and will eventually crash displaying the %SYS-2-WATCHDOG message:

```
*Mar 29 11:29:35.938: %SYS-3-CPUHOG: Task is running for (128004)msecs, more 
than (2000)msecs
(1426/5),process = Virtual Exec.
-Traceback= 0x41DC8E2C 0x41DC9098 0x41BAA6E0 0x41BA6990 0x41B96B4C 0x41BA6768 
0x41BA7490 0x41BA7750
0x41BAC854 0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8 
0x41834200

*Mar 29 11:29:35.942: %SYS-2-WATCHDOG: Process aborted on watchdog timeout, 
process = Virtual Exec.
-Traceback= 0x41A23CC8 0x41BAA3D8 0x41BA6A08 0x41B96B4C 0x41BA6768 0x41BA7490 
0x41BA7750 0x41BAC854
0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8 0x41834200 
0x418341E4

%Software-forced reload
```

  Workaround: Do not initiate SSH or SCP sessions from the router. (CSCsb54378)

- When you remove the **radius-server source-ports 1645-1646** default command, the switch sends the RADIUS requests with the wrong source port, causing the authentication attempts to fail.

  Workaround: Ensure that the **radius-server source-ports 1645-1646** command is configured and reload the switch. Upon boot-up, the command will be in the running-config and communication with the RADIUS server will resume. (CSCsh22161)

- Memory corruption may occur if a EIGRP stub with static routes is configured on the switch, causing the switch to crash. Symptoms include console messages similar to the following:

  ```
  Aug 23 15:43:45: %SYS-2-BADSHARE: Bad refcount in mem_lock, ptr=43258E68,
  count=FFFF8000

  Traceback= 409201A8 4007AE28 40A1D418 40A2263C 40A24610 40A25600 40C309D4 40C30D74
  40C3CBB0CMD:
  ```

  Workaround: Unconfigure the EIGRP stub with static routes. (CSCef26340)

- A memory leak may occur if a switch is configured as a RADIUS client and receives invalid RADIUS packets. The switch will not have enough packet memory to receive incoming ARP packets destined for the CPU, and ARP entries will be incomplete.

  Workaround: Disable the port that is receiving invalid RADIUS packets. (CSCeh84727)

- If the ACL configured on an SVI is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SGA and resize the TCAM with the **access-list hardware region balance** command to support the ACL. Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCsh50565)

- Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS.

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007.

  (CSCsb12598)

- Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007.

(CSCsb40304)

- Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS.

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007.

  (CSCsd92405)

Open Caveats in Cisco IOS Release 12.2(25)EWA8

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA8:

- While configuring Smartport macros via HTTP interactively, a Catalyst 4500 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- A Catalyst 4500 series switch upgrading to IOS versions 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

```
Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
```

This does not impact the operation of the Catalyst 4500 series switch, appearing to be strictly cosmetic.

Workaround: Power-cycle the switch. (CSCsg00796)

- A Catalyst 4500 series switch running Cisco IOS Release 12.(25)EWA8 will send in dot1q tagged cdp packets when dot1x is enabled on a voice VLAN port. This might cause gigabit IP phones to send in packets that are untagged, moving the phone into the data VLAN.

  Workaround: Do either of the following:

  - Remove dot1x from the port.
  - Upgrade the IOS image to Cisco IOS 12.2(31)SGA or later.

  (CSCsg10135)

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

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- If the ACL configured on an SVI is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SGA and resize the TCAM with the **access-list hardware region balance** command to support the ACL. Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCsh50565)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA8

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA8:

In a switch running Cisco IOS Release 12.2(25)EWA8, the following symptoms might be observed.

- ARP does not resolve for directly-connected devices, impacting connectivity and preventing routing protocols from forming an adjacency.
- If UDLD “aggressive” is enabled, ports will err-disable due to UDLD, causing messages like the following to display:

```
%UDLD-4-UDLD_PORT_DISABLED: UDLD disabled interface Gi3/1, unidirectional link
detected
%PM-4-ERR_DISABLE: udld error detected on Gi3/1, putting Gi3/1 in err-disable
state
```

Note Because UDLD is merely a symptom of the problem rather than the cause, disabling UDLD will not solve the problem.

- Slow memory leak, causing messages (with tracebacks) like the following to display:

```
%SYS-2-MALLOCFAIL: Memory allocation of 784 bytes failed from 0xXXXXXX, alignment
8
Pool: Processor  Free: 36  Cause: Not enough free memory Alternate Pool: None
Free: 0  Cause: No
Alternate pool -Process= "<Process_name>", ipl= 0, pid= 49 -Traceback=
0xXXXXXX
```

Messages such as the following would be seen on the console

```
%% Low on memory; try again later
```

If one of the symptoms is observed, capture an output of the **show tech** command along with 4-5 snapshots of the following commands (over a 10 minute interval) and open a TAC Service request:

- **show plat cpu packet driver**
- **show plat cpu pack stat**
- **show platform health**
- **show mem summary**
- **show process memory**

Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA6. (CSCsh25687)

- Starting in calendar year 2007, daylight savings summer-time rules may cause Cisco IOS to generate timestamps (such as in syslog messages) that are off by one hour.

  By default, the Cisco IOS configuration command uses United States standards for daylight savings time rules:

  clock summer-time *zone* **recurring**

  The Energy Policy Act of 2005 (H.R.6.ENR), Section 110 changes the start date from the first Sunday of April to the second Sunday of March, and it changes the end date from the last Sunday of October to the first Sunday of November.

  Workaround: Use the **clock summer-time** command to manually configure the proper start and end date for daylight savings time. After the summer-time period for calendar year 2006 ends, you can configure the following for the US/Pacific time zone:

  clock summer-time *PDT* **recurring** *2 Sun Mar 2:00 1 Sun Nov 2:00*

  (CSCsg70355)

Note Using NTP is not a workaround to this problem, because it does not carry any information about timezones or summertime.

Open Caveats in Cisco IOS Release 12.2(25)EWA7

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA7:

- While configuring Smartport macros via HTTP interactively, a Catalyst 4500 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- A Catalyst 4500 series switch upgrading to IOS versions 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This does not impact the operation of the Catalyst 4500 series switch, appearing to be strictly cosmetic.

  Workaround: Power-cycle the switch. (CSCsg00796)

- A Catalyst 4500 series switch running Cisco IOS Release 12.(25)EWA8 will send in dot1q tagged cdp packets when dot1x is enabled on a voice VLAN port. This might cause gigabit IP phones to send in packets that are untagged, moving the phone into the data VLAN.

  Workaround: Do either of the following:

  - Remove dot1x from the port.
  - Upgrade the IOS image to Cisco IOS 12.2(31)SGA or later.

  (CSCsg10135)

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

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA7

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA7:

- When VRF Packet Leaking is configured on a Catalyst 4500 series switch with a Supervisor Engine IV, a packet loss of 50 per cent occurs when you ping a VRF interface IP address from a device in the global table.

  Packets forwarded by the switch are not impacted.

  Workaround: None. (CSCej36831)

- If you running Cisco IOS Release 12.2(25)EWA5 on a Catalyst 4500 series switch, after reloading an "ip ftp source-interface <physical port>" configuration, it is impossible to upload the configuration to the FTP Server with the **copy running-config ftp** command.

  Workaround: Issue the **ip ftp source-interface <loopback port>** command rather than the **ip ftp source-interface <physical port>** command. (CSCsd22662)

- Reconfiguring a heavily-used policy map on a Catalyst 4500 series switch may cause the switch to crash.

  This issue impacts Cisco IOS Releases 12.2(25)EWA3, 12.2(25)EWA4, 12.2(25)EWA5, 12.2(25)EWA6, 12.2(25)SG and 12.2(31)SG.

  Workaround: Remove the policy-map from all interfaces before reconfiguring its contents. Also ensure that no configuration is made in parallel that might cause concurrent modification of configured interface's state. (CSCse80948)

- Configuring an ACL on a port configured with the **switchport access vlan dynamic** command will cause the Catalyst 4500 series switch to crash.

  This issue impacts Catalyst 4500 series switches running IOS release including and prior to 12.2(31)SGA and 12.2(25)EWA6.

  Workaround: None. (CSCsg03745)

- GARP-based protocol packets leak through the STP block. In a redundant topology, this might lead to a GARP storm.

  Workaround: Use Hardware Control Plane Policing (CoPP) to police GARP packets. (CSCsg08775)

- A reload of a Catalyst 4500 series switch may cause neighbour switches connected over WS-X4448-GE modules to errdisable their links to the switch because of too many link flaps.

Workaround: Configure “errdisable recovery cause link-flap” on the connected switches. (CSCsd55376)

- When the **clear arp snmp** command is sent to a Catalyst 4500 series switch running Cisco IOS Release 12.2(25)EWA4, the switch may reset.

  This issue impacts Catalyst 4500 series switches running IOS releases including and prior to 12.2(31)SG and 12.2(25)EWA6.

  Workaround: None. (CSCse49277)

- When there are numerous non-RPF multicast groups and the incoming rate of multicast traffic is high, the Catalyst 4500 series switch does not trigger a PIM Assert for some multicast groups immediately after receiving multicast packets on non-RPF interface.

  Workaround: None. (CSCse56839)

- While running Cisco IOS Release 12.2(25)EWA6 on either the Catalyst 4500 series switch, the 4013+TS supervisor engine, or the 4306-GB-T linecard, you might experience the following problem on RJ45 ports:

  - At 1Gbps, the ports cannot sustain the linerate when sending packets greater than 6656 bytes.
  - In rare situations, the TxQueue's associated with the RJ45 ports may get stuck when the packets of greater than 6656 bytes are involved and the port is operating at 10Mbps, 100Mbps, or 1Gbps. You would see the following type of messages:

    ```
    Aug  1 04:46:01 CDT: %C4K_HWPORTMAN-4-BLOCKEDTXQUEUE: Blocked transmit queue 
    HwTxQId1
    on Switch Phyport Gi1/35, count=1784
    Aug  1 04:46:12 CDT: Current Freelist count 5629. Fell below threshold 601 times 
    consecutively
    Aug  1 04:46:42 CDT: Current Freelist count 5629. Fell below threshold 1202 times 
    consecutively
    ```

  Workaround: Use packets sizes less than or equal to 6656 bytes or use Cisco IOS Release 12.2(25)EWA5 until the fix is available in subsequent releases. The fix will be available in 12.2(25)EWA7 release onwards. (CSCse29295)

- On a Catalyst 4500 series switch with an IOS-based supervisor engine running Cisco IOS Release 12.2(25)EWA6 or earlier, some linecards may boot as faulty, including:

  - WS-X4448-GB-RJ45,
  - WS-X4448-GB-LX,
  - WS-4448-GB-SFP,
  - WS-X4548-GB-RJ45,
  - WS-X4548-GB-RJ45V,
  - WS-X4424-GB-RJ45,
  - WS-X4524-GB-RJ45V.

  The **show diagnostic result module 2 test all detail** command returns the following:

  ```
  Test results: (. = Pass, F = Fail, U = Untested)

    ___________________________________________________________________________?

     1) linecard-online-diag --------------------> F <<--

           Error code --------------------------> 4 (DIAG_PARTIAL_FAILURE) <<---
           Total run count ---------------------> 1
           Last test execution time ------------> Jul 12 2006 12:11:29
  ```

```
          First test failure time -------------> Jul 12 2006 12:11:29
          Last test failure time --------------> Jul 12 2006 12:11:29
          Last test pass time -----------------> n/a
          Total failure count -----------------> 1
          Consecutive failure count -----------> 1

Slot Ports Card Type                              Diag Status      Diag Details
---- ----- -------------------------------------- ---------------- ------------
 2    48   10/100/1000BaseT (RJ45)V, Cisco/IEEE   Partial Failure  Port failure

Detailed Status
---------------
. = Pass              U = Unknown
L = Loopback failure  S = Stub failure
I = Ilc failure       P = Port failure
E = SEEPROM failure   G = GBIC integrity check failure


Ports 1   2   3   4   5   6   7   8   9   10  11  12  13  14  15  16
      S   S   S   S   S   S   S   S   .   .   .   .   .   .   .   .

Ports 17  18  19  20  21  22  23  24  25  26  27  28  29  30  31  32
      .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .

Ports 33  34  35  36  37  38  39  40  41  42  43  44  45  46  47  48
      .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .
<snip>
```

You can verify the failure by looking at the output of the **show platform software interface** <*failed_port*> **stub internal** command for any of the faulty ports. The output should include the following:

```
Lemans 2-1(Gi2/1-8) Statistics for Port 0
Symbol Error Counter Reg 0          : 0xFFFFFFFFFFFFFFFF
Symbol Error Counter Reg 1          : 0xFFFFFFFFFFFFFFFF
Symbol Error Counter Reg 2          : 0xFFFFFFFFFFFFFFFF
Symbol Error Counter Reg 3          : 0xFFFFFFFFFFFFFFFF
Symbol Error Counter Reg 4          : 0x0000FFFFFFFF0000
Pause Frame Invalid Opcode Reg 0    : 0xFFFFFFFFFFFFFFFF
Pause Frame Invalid Opcode Reg 1    : 0xFFFFFFFFFFFFFFFF
Pause Frame Invalid Opcode Reg 2    : 0xFFFFFFFFFFFFFFFF
Pause Frame Invalid Opcode Reg 3    : 0xFFFFFFFFFFFFFFFF
Transmit No Buffer Reg 0            : 0xFFFFFFFFFFFFFFFF
Transmit No Buffer Reg 1            : 0xFFFFFFFFFFFFFFFF
Transmit No Buffer Reg 2            : 0xFFFFFFFFFFFFFFFF
Transmit No Buffer Reg 3            : 0xFFFFFFFFFFFFFFFF
```

If the Symbol Error Count Reg 4 is NOT *0xFFFFFFFFFFFFFFFF* then the faulty condition can be attributed to this bug.

Workaround: Reset the module’s status with the **hw-module module reset** command. (CSCse80413)

- If a Catalyst 4500 series switch running Cisco IOS Release 12.2(31)SG is configured with Port Security and Cisco IP Phones are connected to the switchports, the CPU might be higher than expected. In the output of the **show platform health** command, the process hogging the CPU would be the following

```
CAT4506#sh platform health | inc K2L2 Address
K2L2 Address Table R   2.00  27.08     12      5  100  500   15  23   19  4871:26
CAT4506##sh platform health | inc K2L2 Address
K2L2 Address Table R   2.00  34.92     12      5  100  500   38  25   19  4871:32
```

This process should not cause any forwarding issues.

Workaround: None. (CSCse72353)

- Reading the object dot1dTpLearnedEntryDiscards always returns zero.

  Workaround: None. (CSCse66318)

- Applying an ACL to a Layer 3 interface on a Catalyst 4500 series switch that is too large to fit entirely in the TCAM, might cause valid arp replies to be installed incorrectly.

  Workaround: Determine which portion of the TCAM is becoming saturated and resize it accordingly. This can be done by looking at the output of the **show plat hard acl statistics u brief** command:

```
                         Entries/Total(%)  Masks/Total(%)
                           -----------------   ---------------
Input  Acl(PortAndVlan)     5 / 8112 (  0)     3 / 1014 (  0)
Input  Acl(PortOrVlan)   8105 / 8112 ( 99)  1014 / 1014 (100)
Input  Qos(PortAndVlan)     0 / 8128 (  0)     0 / 1016 (  0)
Input  Qos(PortOrVlan)      0 / 8128 (  0)     0 / 1016 (  0)
Output Acl(PortAndVlan)     0 / 8112 (  0)     0 / 1014 (  0)
Output Acl(PortOrVlan)      5 / 8112 (  0)     3 / 1014 (  0)
Output Qos(PortAndVlan)     0 / 8128 (  0)     0 / 1016 (  0)
Output Qos(PortOrVlan)      0 / 8128 (  0)     0 / 1016 (  0)
```

  On a Catalyst 4500 series switch running Cisco IOS Release 12.2(31)SG or later, you can reize the TCAM allocation with the **access-list hardware region** [**feature/qos**] **in balance [***percentage***]** command. (CSCse53198)

- Upon reloading a Catalyst 4500 series switch configured with the **ip ftp source-interface** <*physical port*> command and running Cisco IOS Release 12.2(25)EWA5, it is impossible to upload a configuraton to the FTP Server by issuing the **copy running-config ftp** command.

  Workaround: Issue the **ip ftp source-interface** <*loopback port*>, instead of the **ip ftp source-interface** <*physical port*> command. (CSCsd22662)

- When a “shut/no shut” is performed on some ports of a Catalyst 4500 series switch, an adjacent port might drop some packets (less than 20).

  Workaround: Upgrade to Cisco IOS Release 12.2(25)EWA7 or later. (CSCsg02099)

- The link between WS-X4548-GB-RJ45 and WS-C3560-24PS might not come up (that is, both interfaces stay down) after reloading a Catalyst 4500 series switch with Supervisor Engine IV running Cisco IOS Release 12.2(25)EWA5 or 12.2(25)SG.

  This problem is not seen when WS-C3560-24PS is reloaded.

  Workaround: Do a “shut/no shut” on the interface. (CSCsd90837)

- A Catalyst 4500 series switch running Cisco IOS Release 12.2(25)EWA6, drops some ARP request packets in some VLANs.

  Workaround: None. (CSCsf16422)

- Ports on a WS-X4418-GB in a Catalyst 4500 switch may come up in half-duplex after the link is reset. This symptom is accompanied by logging duplex mismatch messages.

  The problem has been seen with connections between a WS-X4418-GB module and a Catalyst 3550 series switch, a Catalyst 3560 series switch, and a Catalyst 3500xl series switches.

  Workaround: Do a "shut/no shut" on the interface on WS-X4418-GB. (CSCsg21514)

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  (CSCsd75273)
- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  (CSCse52951)

Open Caveats in Cisco IOS Release 12.2(25)EWA6

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA6:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)
- While configuring Smartport macros via HTTP interactively, a Catalyst 4500 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)
- When VRF Packet Leaking is configured on a Catalyst 4500 series switch with a Supervisor Engine IV, a packet loss of 50 per cent occurs when you ping a Catalyst 4500 series switch VRF interface IP address from a device in the global table.

  Packets forwarded by Catalyst 4500 series switch are not impacted.

  Workaround: None. (CSCej36831)

- When you insert gbics on a WS-X4448-GB-SFP running Cisco IOS Release 12.2(25)EWA2 on a WS-C4610R chassis, the output of **show interface status** and **show interface** displays "media type is No Gbic".

  Workaround: OIR the WS-X4448-GB-SFP. (CSCsd57960)
- While running Cisco IOS Release 12.2(25)EWA5, after reloading an "ip ftp source-interface <physical port>" configuration, it is impossible to upload the configuration to the FTP Server with the **copy running-config ftp** command.

  Workaround: Issue the **ip ftp source-interface <loopback port>** command rather than the **ip ftp source-interface <physical port>** command. (CSCsd22662)
- An active supervisor engine WS-X4516-10GE in a WS-C4510R chassis running Cisco IOS Release 12.2(25)EWA2 crashes when you replace the standby supervisor engine WS-X4516-10GE.

  Workaround: None. (CSCsd46408)
- When a third-party device is connected to a 1000BaseX interface and the link is shutdown/unshutdown, the autonegotiation process takes considerable time to complete and the link needs several minutes to come up again.

  Workaround: Disable autonegotiation or flow-control. (CSCse33607)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA6

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA6:

- On a Supervisor Engine V10-GE, when there are lot of flows in the system, an error message is logged to SYSLOG indicating that the netflow hardware table is full. The error message is misleading; the message states "flow table full" instead of "flow collisions."

  Workaround: None. (CSCeh97868)
- Occasionally, when a Catalyst 4500 series switch is in VTP client mode and “switchport trunk prunning vlan none” is configured on the trunk port, the trunk interface fails to send VLAN joins to the VTP server. Some of the VLAN is pruned on the link to the VTP server even when those VLANs are used.

  Workaround: Instead of using the "none" option, provide a specific VLAN when enabling VTP pruning on the trunk interface. (CSCei42957)
- After you initially boot a Catalyst 4500 series switch, if the input interface is in PIM dense mode, “s,g” multicast cast traffic is not forwarded to the intended destination even if that group is represented by a “*,g” on the system.

  Workaround: Issue the **clear ip mroute *** command multiple times. (CSCsb50317)
- A standby Supervisor Engine IV in SSO mode might restart in a Catalyst 4507R series switch running Cisco IOS Release 12.2(25)EWA.

  Workaround: None. (CSCsc41651)
- When PVLAN features (for example, PVLAN QoS) are applied on a trunk port for a number of VLANs and later removed from some VLANs, the features may be reprogrammed for all other VLANs. While the reprogramming is in progress, you might see some log message indicating that the features could not be programmed for some of the VLANs.

  Workaround: Remove the features and reapply. For PVLAN QoS, issuing a **no qos** and **qos** command will help. (CSCsc61449)

- On Cisco IOS Release 12.2(25)EWA4 and 12.2(25)EWA5, the system may crash during modification of a policy map attached to an interface with the **set ip {dscp|ip|precedence}** command.

  Workaround: Remove the policy-map from the interface and re-configure a new policy-map without this option. (CSCsc97186)

- On a WS-C4948 running Cisco IOS Release 12.2(25)EWA3, you cannot re-set the interface MTU to the default.

  Workaround: Return the value of "Global Ethernet MTU" to the previous default value. (CSCsb81150)

- The following error messages may appear on a Catalyst 4500 series switch after reload, causing it to lose its VLAN configuration and preventing you from recreating them:

  This is observed on a switch whose VTP is in transparent mode, Version 2, after some non-default settings for VLANs 1003 and 1005 (token ring) were learned when the switch was in server mode.

  ```
  %SW_VLAN-4-VTP_INTERNAL_ERROR: VLAN manager received an internal error 14 from vtp
  function vtp_download_info: Bad parent VLAN ID-Traceback=...
  ```

  Workarounds:

  - Return to VTP version 1.
  - Use a 'ring' value in the range for 1 - 1005 for all Token Ring VLANs (CSCsc69560)

- When you configure “logging host X.X.X.X vrf,” on a WS-X4515 chassis that is running Cisco IOS Release 12.2(25)EWA5 or 12.2(25)SG, the chassis does not accept the command line to delete this configuration.

  Workaround: Issue the **erase start** command. (CSCek33573).

- If a physical interface is configured in shutdown mode, then configured with the same configuration including "switchport nonegotiate,” when it is later enabled by the **no shutdown** command, it can not join the bundle and the following error message displays:

  ```
  %EC-5-CANNOT_BUNDLE2: Gi3/16 is not compatible with Po1and will be suspended (trunk
  mode of Gi3/16 is dynamic, Po1 is trunk)
  ```

  The following configuration sequence will prevent interface g3/16 from joining the bundle:

  ```
  int g3/16
  shut
  switchport mode trunk
  switchport nonegotiate
  channel-group 1 mode on

  int po1
  switchport trunk enacp dot1q
  switchport mode trunk
  switchport nonegotiate

  int g3/16
   no shut
  ```

  Workaround: Do NOT configure the channel-port with the same configuration while all physical ports are still in shutdown mode. Instead, issue the **unshutdown** command on the physical ports to carry over the first unshutdown to the channel port. (CSCsd11234)

- When you set up a topology wherein a Catalyst 6000 series switch is connected by multiple links to Port 2, 15-16, 21-47 of a Catalyst 4948 series switch, after 1 minute, the blocking port of Catalyst 4948 starts flapping the STP port status.

Workaround: Shutdown 2 ports to reduce the number of VLAN instances. (CSCsc29392)

- On a Catalyst 4500 series switch running Cisco IOS Release 12.2(25)EWA2, dhcp snooping does not work on a PVLAN trunk.

  Workaround: None (CSCej06004).

- The first multicast packet is dropped.

  Workaround: None (CSCsc51906).

- The BOOT variable is not cleared with the **no boot system** command.

  Workaround: Check the variable with the **show bootvar** command before issuing the **write memory** command. (CSCeg74620).

- For Cisco IOS Releases preceeding Cisco IOS 12.2(25)EWA6, if the Inline Power circuit of a 4200W power supply fails, the supervisor engine might not switchover to the Active power supply. This will cause a IP phone outage because the Inline power drops to zero. This problem can occur in redundant mode or combined mode.

  Workarounds:

  - Remove the failed power supply from the bay.
  - Upgrade to Cisco IOS Release 12.2(25)EWA6 or releases after Cisco IOS Releases 12.2(31)SG. (CSCse18104)

- If an interface is set to “not autonegotiate” from SNMP, and an snmp get is done to query the state of the interface, the correct state is returned. However, if the interface is set to “not autonegotiate” from the CLI, then an snmp get will show that it is still in autonegotiate mode, even though it isn't.

  Workaround: If the autonegotiate state is set by SNMP through the ifMauAutoNegAdminStatus value, it is reported by SNMP and CLI correctly. (CSCsc21274).

- After an SSO switchover, a Catalyst 4500 series switch running in Cisco IOS Releases 12.2(20)EWA to 12.2(20)EWA3, 12.2(25)EW, and 12.2(25)EWA to 12.2(25)EWA5, the Fantray index is missing the entPhysicalTable of the entity MIB.

  Workaround: None. (CSCei17285).

- When copying files to and from the switch, using ftp, the operation fails for files larger than 18528 bytes when the ftp server is on a remote network.

  A sample operation is:

  ```
  switch# copy running-conf ftp://user:password@n.n.n.n//users/xxx/switch-confg
  ```

  The error is:

  ```
  00:02:06: FTP: 550 /users/xxx/switch-confg: Broken pipe.
  ```

  Workaround: Either use a local ftp server on the same network or use tftp or rcp. (CSCsc48710).

- You might be the continuous error messages like:

  ```
  Dec 19 10:53:36: %C4K_PKTPROCESSING-4-UNKNOWNBRIDGEORROUTE: (Suppressed 52 times)
  Unable to determine whether to route or bridge replicated software-processed pa cket
  with source address 00:04:AC:E4:BC:38 and destination address 00:00:0C:07:AC:23

  Dec 19 11:03:45: %C4K_PKTPROCESSING-4-UNKNOWNBRIDGEORROUTE: (Suppressed 48 times)
  Unable to determine whether to route or bridge replicated software-processed packet
  with source address 00:04:AC:E4:BC:38 and destination address 00:00:0C:07:AC:23

  Dec 19 11:13:52: %C4K_PKTPROCESSING-4-UNKNOWNBRIDGEORROUTE: (Suppressed 37 times)
  Unable to determine whether to route or bridge replicated software-processed pa cket
  with source address 00:04:AC:E4:BC:38 and destination address 00:00:0C:07:AC:23
  ```

Workaround: None (CSCsc87365).

- On a WS-X4306 on Catalyst WS-C4507R running 12.2(25)SG and 12.2(25)EWA5, after configuring “speed nonegotiate" in interface range, Symbol-Err and Sequence-Err counters increase.

  Workaround: Link up these ports through the **no shutdown** command. (CSCsc71324).

- Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  (CSCek26492)

- The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177.

  There are workarounds available to mitigate the effects of the vulnerability.

  (CSCek37177)

- Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  (CSCsd40334)

- Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  (CSCsd58381)

Open Caveats in Cisco IOS Release 12.2(25)EWA5

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA5:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- After moving to a non-redundant chassis, a supervisor engine previously configured in SSO mode cannot configure router ports or port-channel.

  Workarounds:

  - 1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR.
  - 2. Enter the **write memory** command and reload the switch from the non-redundancy chassis. (CSCef67677)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, and then the **no shutdown** command on the same port ensures that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- A QoS policing fails if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers. (CSCsa57218)

- On a Supervisor Engine V10-GE, when there are lot of flows in the system, an error message is logged to SYSLOG indicating that the netflow hardware table is full. The error message is misleading; the message states "flow table full" instead of "flow collisions."

  Workaround: None. (CSCeh97868)

- Occasionally, when a Catalyst 4500 series switch is in VTP client mode and “switchport trunk prunning vlan none” is configured on the trunk port, the trunk interface fails to send VLAN joins to the VTP server. Some of the VLAN is pruned on the link to the VTP server even when those VLANs are used.

  Workaround: Instead of using the "none" option, provide a specific VLAN when enabling VTP pruning on the trunk interface. (CSCei42957)

- While configuring Smartport macros via HTTP interactively, a Catalyst 4500 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsc05612)

- When VRF Packet Leaking is configured on a Catalyst 4500 series switch with a Supervisor Engine IV, a packet loss of 50 per cent occurs when you ping a Catalyst 4500 series switch VRF interface IP address from a device in the global table.

  Packets forwarded by Catalyst 4500 series switch are not impacted.

  Workaround: None. (CSCej36831)

- On a Catalyst 4500 series switch running Cisco IOS Release 12.2(18)EW2 or 12.2(18)EW5, instances of the entAliasMappingIdentifier MIB object for some interfaces are missing. This situation can occur randomly on interfaces, regardless of their type, location and status.

  Workaround: None. (CSCsc07093)

- After you initially boot a Catalyst 4500 series switch, if the input interface is in PIM dense mode, “s,g” multicast cast traffic is not forwarded to the intended destination even if that group is represented by a “*,g” on the system.

  Workaround: Issue the **clear ip mroute *** command multiple times. (CSCsb50317)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA5

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA5:

- On the WS-4948G (RJ45 and SFP ports), WS-4948G-10GE (RJ45 ports only), WS-X4506-GB-T (RJ45 ports only), and WS-X4013+TS (RJ45 ports only), one or more ports may exhibit complete loss of traffic in both the transmit and receive directions. The problem can be seen on a port when its link flaps (up/down) multiple times in a short period of time.

  This problem impacts all IOS releases starting from Cisco IOS Release 12.2(25)EWA2 or later, including 12.2(25)SG. Entering the **shut** and **no shut** commands will not recover from this problem.

  Please verify the following problem conditions to confirm the occurrence of this problem:

  - Issue the **show interface** *module/port* **status** command; it displays the Connected state
  - Issue the **show platform hardware interface GigabitEthernet** *module/port* **all**; it indicates that the MAC state is “Down” and that the rxInReset flag is set to “True”

  Workaround: Reload the switch. (CSCsc10017)

- A WS-4948G, WS-4948G-10GE, WS-X4506-GB-T, and WS-X4013+TS might display the following message while running the Cisco IOS Release 12.2(20)EWA and later:

  ```
  %C4K_HWPORTMAN-4-BLOCKEDTXQUEUE: Blocked transmit queue HwTxQId1 on Switch Phyport
  18,count=342141
  ```

  Ports with a duplex mis-match and the switch port operating in half duplex will exhibit this problem and no traffic will flow through those ports.

  Such a mis-match can occur when the switch port is configured for auto-negotiation but the far-end device is operating in forced mode. This mis-match can also occur when both ends of the link are operating in forced mode with the same speed but different duplex settings.

  Workarounds:

  - Issue shut /no shut to recover the port. (Prior to Cisco IOS Release 12.2(25)EWA2, a reload may be required.)
  - Repair the duplex mis-match. Ensure that both the switch and the far-end device are both auto-negotiating or forced to operate at same speed and duplex. (CSCsb62330)
- A Catalyst 4500 series switch does not forward an 802.1X request with NULL credentials.

  Workaround: None. (CSCej03858)
- A port enabled for Loop Guard that participates in spanning tree (and is in BLK state) goes into a loop inconsistent state when it stops receiving BPDUs from its neighbor. When the neighbor resumes sending BPDUs (instead of STP BPDUs), STP ordinarily recovers from this state. For this caveat, STP does not recover and the port remains stuck.

  Workarounds:

  - Enter the **shut** and **no shut** commands on the port.
  - Disable Loop Guard on the port and then re-enable it. (CSCsc04047)
- A Catalyst 4500 series switch with Supervisor Engine IV running Cisco IOS Release 12.2(25)EWA3 will send an ARP packet (from an STP blocking port) that can cause a broadcast storm when you either reload a Catalyst 4500 series switch with a blocking port or enter **shut** and **no shut** commands on any port of the switch.

  Workaround: None. (CSCsb84685)
- If UDLD is enabled on a trunk port with native VLAN tagging enabled, the UDLD protocol packets are sent out untagged. This may cause UDLD interoperability issues with other Cisco switches that expect to always see tagged packets on trunk ports.

  Workaround: None. (CSCsb34771)

Open Caveats in Cisco IOS Release 12.2(25)EWA4

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA4:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

```
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- After moving to a non-redundant chassis, a supervisor engine previously configured in SSO mode cannot configure router ports or port-channel.

  Workarounds:

  - 1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR.
  - 2. Enter the **write memory** command and reload the switch from the non-redundancy chassis. (CSCef67677)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, and then the **no shutdown** command on the same port ensures that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature shows only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands are accepted, even after you enter the **macro apply** command. (CSCsa44632)

- QoS policing fails if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers. (CSCsa57218)

- After you initially boot a Catalyst 4500 series switch, if the input interface is in PIM dense mode, "s,g" multicast cast traffic is not forwarded to the intended destination even if that group is represented by a "*,g" on the system.

  Workaround: Issue the **clear ip mroute *** command multiple times. (CSCsb50317)

- On a Supervisor Engine V10-GE, when there are lot of flows in the system, an error message is logged to SYSLOG indicating that the netflow hardware table is full. The error message is misleading; the message states "flow table full" instead of "flow collisions."

  Workaround: None. (CSCeh97868)

- Occasionally, when a Catalyst 4500 series switch is in VTP client mode and "switchport trunk prunning vlan none" is configured on the trunk port, the trunk interface fails to send VLAN joins to the VTP server. Some of the VLAN is pruned on the link to the VTP server even when those VLANs are used.

Workaround: Instead of using the "none" option, you must provide a specific VLAN when enabling VTP pruning on the trunk interface. (CSCei42957)

- If UDLD is enabled on a trunk port with native VLAN tagging enabled, the UDLD protocol packets are sent out untagged. This may cause UDLD interoperability issues with other Cisco switches that expect to always see tagged packets on trunk ports.

  Workaround: None. (CSCsb34771)

- While configuring Smartport macros via HTTP interactively, a Catalyst 4500 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA4

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA4:

- Issuing the **no ip flow ingress** command does not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command.

  (CSCsa67042)

- Modifying a policer may not work if you configure more than 800 policers.

  Workaround: Remove, reconfigure and reinstall policers, or, use less than 800 policers. (CSCsa66422)

- The **dot1x default** command does not restore the defaults for the **dot1x max-reauth-req** and **dot1x timeout reauth server** commands.

  Workaround: Restore these default values manually. (CSCeh97513)

- During an SSO switchover, if another device telnets to a Catalyst 4500 series switch while this switch is in global configuration mode, you might observe the following with the **show users** command:

```
4507R# show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                idle                 00:00:00
   1 vty 0                idle                    never  <<<==========
```

  After vty is set to “never,” it cannot be released with the **clear line XX** command.

  Workaround: Reload the system. (CSCei26830)

Note Always exit the global configuration mode *before* a switchover.

- After changing the SNMP engine ID on a Catalyst 4500 series switch running Cisco IOS Release 12.2(25)EWA, none of the existing community strings work. You must re-establish the relationship between any community strings and the new engine ID.

  Upon issuing the **snmp mib community-map** command, you will observe additional SNMP configuration entries that reflect the mismatched SNMP engine ID.

  Workaround: Remove the community-map with the **no snmp mib community-map** command. (CSCei29841)

- With IP multicast routing and IGMP snooping enabled, a Catalyst 4500 series switch does not send ARP requests to a partner switch if the trunk port on the Catalyst 4500 switch is the only interface carrying private VLANs.

  Workaround: Configure any other port on the Catalyst 4500 switch (not necessarily one connected to the partner switch) as a regular trunk interface. Ensure that the interface is "link up" and carries both primary and isolated VLANs. (CSCsb06924)

- After executing a redundancy force-switchover, a Catalyst 4500 series switch loaded with a redundant supervisor engine may reload when you issue a **show snmp group** command.

  Workaround: None. (CSCsb12225)

- If an 802.1X supplicant logs off, the AAA Accounting Stop record displays "port-error" as the Acct-Terminate-Cause[49] reason instead of "user-req."

  Workaround: None.(CSCsb36480)

- A Catalyst 4500 series switch running the Cisco IOS Release 12.2(25)EWA2 does not send LinkUp traps (IF-MIB).

  Workaround: Issue the **snmp trap link-status permit duplicates** command on the interfaces. (CSCsb38308)

Note Do not use this command with redundant supervisor engines because its behavior at switchover is unpredictable. Moreover, it does not work with the **interface range** command; configure the command on every interface.

- When there are two supervisor engines in a redundant Catalyst 4500 chassis, the active supervisor engine reloads when you configure the following:

  ```
  router bgp 100
  bgp upgrade-cli
  ```

  Workaround: Do not issue the **bgp upgrade-cli** command on a redundant chassis. (CSCsb42734)

- Executing the **show** command in trustpoint-ca configuration mode might cause the switch to fail by corrupting the stack.

  Workaround: Do not issue the **show** command in trust-ca configuration mode. (CSCsb42958)

- When 802.1X accounting is enabled, the Framed-IP-Address[8] attribute is not included in accounting messages generated on ports with IP DHCP snooping trust enabled.

  Workaround: None. (CSCsb46019)

- If storm control is configured and you manually toggle the link (up/down), the ARP table no longer updates its database.

  Workaround: Allow storm control to disable and enable the interface. (CSCsb49409)

- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  (CSCei61732)

- Symptoms: The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally-exploitable buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error.

  Conditions: The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

  Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759—VTP version field DoS
  - CSCse40078/CSCse47765—Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

  (CSCei54611)

Open Caveats in Cisco IOS Release 12.2(25)EWA3

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA3:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This activity can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- After moving to a non-redundant chassis, a supervisor engine that was previously configured in SSO mode will not be able to configure router ports or port-channel.

  Workarounds:

  1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR.

  2. Enter the **write memory** command and reload the switch from the non-redundancy chassis. (CSCef67677)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   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)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsa44632)

- Under certain rare scenarios, the packet match counter in **show policy-map interface fa6/1** does not show the packets being matched, as in the following configuration:

```
 clearwater#sh policy-map int
  FastEthernet6/2

   Service-policy output: p4

     Class-map: ipc2 (match-all)
       0 packets<---------- It shouldn't stay at '0'.
       Match: access-group name ipacl_2
       police: Per-interface
         Conform: 22937970 bytes Exceed: 977688712 bytes <--- traffic going thru


     Class-map: class-default (match-any)
       410 packets
       Match: any
         410 packets
```

  Workaround: Either enter a shutdown/no shutdown on the port or detach and reapply the service policy. (CSCef30883)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- Issuing the **no ip flow ingress** command will not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command.

  (CSCsa67042)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- Modifying a policer may not work if you configure more than 800 policers.

  Workaround: Remove, reconfigure and reinstall policers, or, use less than 800 policers. (CSCsa66422)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA3

This section lists the resolved caveats in Release 12.2(25)EWA3:

- Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability. (CSCei76358)
- When a Catalyst 4510 series switch is booted with more than 5 WS-X4148-RJ45V (and possibly other PoE) line cards, the supervisor engine occasionally reloads. With 7 WS-X4148-RJ45V line cards, this occurs about 20 per cent of the time.

  Workaround: Because this only occurs around 20 per cent of the time, simply reboot the switch. After the switch boots, this problem will not occur. (CSCsa96753)

Open Caveats in Cisco IOS Release 12.2(25)EWA2

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA2:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)
- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)
- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This activity can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)
- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)
- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- After moving to a non-redundant chassis, a supervisor engine that was previously configured in SSO mode will not be able to configure router ports or port-channel.

  Workarounds:

  1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR.

  2. Enter the **write memory** command and reload the switch from the non-redundancy chassis. (CSCef67677)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   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)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsa44632)

- Under certain rare scenarios, the packet match counter in **show policy-map interface fa6/1** does not show the packets being matched, as in the following configuration:

```
clearwater#sh policy-map int
 FastEthernet6/2

  Service-policy output: p4

    Class-map: ipc2 (match-all)
      0 packets<---------- It shouldn't stay at '0'.
      Match: access-group name ipacl_2
      police: Per-interface
        Conform: 22937970 bytes Exceed: 977688712 bytes <--- traffic going thru


    Class-map: class-default (match-any)
      410 packets
      Match: any
        410 packets
```

  Workaround: Either enter a shutdown/no shutdown on the port or detach and reapply the service policy. (CSCef30883)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- Issuing the **no ip flow ingress** command will not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command.

  (CSCsa67042)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- Modifying a policer may not work if you configure more than 800 policers.

  Workaround: Remove, reconfigure and reinstall policers, or, use less than 800 policers. (CSCsa66422)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA2

This section lists the resolved caveats in Release 12.2(25)EWA2:

- If the switch receives an unlearned source MAC address after a security violation, memory is consumed in creating a security violation-related SNMP trap for each source MAC address. If the switch receives several unlearned source MAC addresses at a very high rate, considerable memory is consumed to ensure that the SNMP traps are generated and sent out correctly.

  Workaround: Configure the trap-rate to limit very small number of traps every second. The following configuration sets a trap-rate of 1/2 trap per second (CSCeg41478):

  ```
  Switch(config)#snmp-ser enable traps port-se trap-rate 1
  Switch(config)#snmp-ser enable traps port-se trap-rate 2
  ```

- If you configure a SPAN session and then apply a SPAN ACL filter to the session, the packets that should be dropped according to the ACL definition are still sent out the SPAN destination port.

  For example, the intent of the following command sequence is to drop packets with source or destination IP address 20.4.1.2 on the SPAN destination port Gigabit Ethernet 6/5:

  ```
  Switch(config)# access-list 1 deny 20.4.1.2
  Switch(config)# monitor session 1 source interface gi6/5
  Switch(config)# monitor session 1 destination interface gi6/7
  Switch(config)# monitor session 1 filter ip access-group 1
  ```

  However, if this is the first time you are applying the ACL filter to the SPAN session, the packets with IP address 20.4.1.2 are still copied to the SPAN destination port.

  If this sample configuration is contained in the startup-config, then the ACL filter would work properly after the Catalyst 4500 series switch boots.

  This caveat only impacts Cisco IOS Release 12.2(25)EWA.

  Workaround: Remove the ACL filter and then re-apply it using the following command sequence:

  ```
  Switch(config)# no monitor session 1 filter ip access-group 1
  Switch(config)# monitor session 1 filter ip access-group 1
  ```

  (CSCsa64231)

- Issuing the **no ip flow ingress** command will not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command.

  (CSCsa67042)

- When you use the **vlan** command in interface range configuration mode to configure a range of VLANs on Layer 3 ports, the VLANs might not be created, as in the following example. Additional VLANs will not be created on the Catalyst 4500 series switch until the switch has been reloaded.

  ```
  Switch(config)# int range gi3/3 - 28
  Switch(config-if-range)# sw
  Switch(config-if-range)# no sw
  Switch(config-if-range)# vlan 1000-4094
  % Command failed on interface GigabitEthernet3/4. Aborting
  Switch(config)#
  ```

  Workaround: Create the VLANs in global or interface command mode. CSCsa54831)

- Deleting the trusted boundary configuration from a port that does not have a phone attached to it and which was configured using the **auto qos voip cisco** command leaves the port in an untrusted state. The **auto qos voip cisco** command will configure two CLI's on a port: **qos trust cos** and **qos trust device cisco-phone**. Removing the **qos trust device cisco-phone** command (using the **no qos trust cisco-phone** command) will cause the port to remain in an untrusted state.

  Workaround: None.(CSCsa64726)

- Under load conditions, the CPU utilization reported on a Catalyst 4500 series switch running Cisco IOS Release 12.2(25)EWA2 is approximately 5 per cent higher than that reported on previous releases of IOS.

  Workaround: In previous releases of Cisco IOS, CPU utilization was computed incorrectly. This defect has been fixed in Cisco IOS Release 12.2(25)EWA2 resulting in slightly higher CPU utilization being reported under similar load conditions as compared to previous releases. (CSCsb19391)

  This is not a problem and a workaround is unnecessary.

- When the active supervisor engine on a Catalyst 4500 series switch redundant chassis is running Release 12.1-based IOS and the standby supervisor engine is running 12.2-based IOS, the following IPC error is seen, and the active supervisor engine is reset by the standby supervisor engine:

```
00:00:36: %C4K_REDUNDANCY-4-KEEPALIVE_WARNING: Keepalive messages from peer Supervisor
are missing for 27 seconds
00:00:38: %CHKPT-3-IPCSESSION: Unable to open an IPC session for communicating with
(STANDBY). rc= 12
00:01:03: %C4K_REDUNDANCY-4-KEEPALIVE_WARNING: Keepalive messages from peer Supervisor
are missing for 54 seconds
00:01:30: %C4K_REDUNDANCY-4-KEEPALIVE_WARNING: Keepalive messages from peer Supervisor
are missing for 81 seconds
00:05:42: %C4K_REDUNDANCY-3-PEER_RELOAD: The peer Supervisor is being reset because
keepalive message(s) not received.
00:05:42: %C4K_REDUNDANCY-6-SWITCHOVER: Switchover activity detected, changing role
from STANDBY to ACTIVE
```

  Workaround: This is not a supported configuration. Ensure that both supervisor engines are running the same IOS release. (CSCsb21892)

- A QoS service-policy cannot be attached to a port or VLAN if routing is not configured on the system.

  Workaround: Enable IP routing on the system, but do not configure any SVIs and or physical routed ports. The routing operation is performed only when a SVI and or physical routed port is configured with a valid IP address. (CSCsa54215)

- When you configure numerous per-port per-VLAN QoS (like 800 input policers), and then modify them, per-port per-VLAN QoS will stop working.

  Workaround: Disable and or re-enable QoS. (CSCsa66422)

- Occasionally, when IPX ACL is configured with a tunnel interface to carry IPX traffic, the Catalyst 4500 series switch reloads once you delete the interface.

  This caveat does not occur in earlier releases.

  Workaround: None. (CSCsa68817)

- Let’s assume that you configure the WS-X4548-GB-RJ45V linecard with the **interface range** command, as follows:

```
power inline static max 15400
no switchport
```

You might receive the following error message-related trace back for any of the configured interfaces within the range:

```
1d02h: %INTERFACE_API-3-NOADDSUBBLOCK: The SWIDB subblock named UDLD was not added to
GigabitEthernet#/#
-Traceback= 1022E35C 10291A1C 1055FE5C 103E3890 103E3924 1038D228 103EF2C8 103EF758
1043D910 101E1B90 103BA750 101E0DA4 101E0858 101FA910 1030F04C 103059E8
```

Workarounds: To avoid the error message, do either of the following:

1. Enter the configuration as soon as the WS-X4548-GB-RJ45V linecard is inserted into the chassis rather than wait for a timeout period.

2. Use interface configuration instead of interface range configuration. (CSCsb24491)

- When a redundant Catalyst 4500 chassis operating in SSO mode is configured for dot1q trunk and performs a switchover, IP traffic might not be able to travel from the Layer 3 interface on the new active supervisor engine to the Layer 3 interface on an interconnected WS-4014.

  Workaround: Clear the arp cache on both supervisor engines. (CSCsb24611)

- Moving a GBIC from one port (uplink or non-uplink) to another may cause a traceback. This problem can occur on any supervisor engine in any Catalyst 4500 chassis.

  Workaround: Ensure that the port is administratively shutdown before you remove the GBIC. (CSCsa66349)

Open Caveats in Cisco IOS Release 12.2(25)EWA1

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA1:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This activity can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- After a supervisor engine switchover in SSO mode, the Diagnostic Optical Monitoring feature (CLI and MIB support) might not work as expected. The **show interfaces transceiver** command will not display any output.

  Workaround: Reload the supervisor engines. (CSCef67309)

- After moving to a non-redundant chassis, a supervisor engine that was previously configured in SSO mode will not be able to configure router ports or port-channel.

  Workarounds:

  1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR.

  2. Enter the **write memory** command and reload the switch from the non-redundancy chassis. (CSCef67677)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   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)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsa44632)

- If the switch receives an unlearned source MAC address after a security violation, memory is consumed in creating a security violation-related SNMP trap for each source MAC address. If the switch receives several unlearned source MAC addresses at a very high rate, considerable memory is consumed to ensure that the SNMP traps are generated and sent out correctly.

  Workaround: Configure the trap-rate to limit very small number of traps every second. The following configuration sets a trap-rate of 1/2 trap per second (CSCeg41478):

```
Switch(config)#snmp-ser enable traps port-se trap-rate 1
Switch(config)#snmp-ser enable traps port-se trap-rate 2
```

- Under certain rare scenarios, the packet match counter in **show policy-map interface fa6/1** does not show the packets being matched, as in the following configuration:

```
 clearwater#sh policy-map int
  FastEthernet6/2

   Service-policy output: p4

     Class-map: ipc2 (match-all)
       0 packets<---------- It shouldn't stay at '0'.
       Match: access-group name ipacl_2
       police: Per-interface
         Conform: 22937970 bytes Exceed: 977688712 bytes <--- traffic going thru


     Class-map: class-default (match-any)
       410 packets
       Match: any
         410 packets
```

Workaround: Either enter a shutdown/no shutdown on the port or detach and reapply the service policy. (CSCef30883)

- When a switchport configured with port security is converted from an access to a promiscuous port, the port security configuration is lost. The **show interface** command will show that port security is no longer configured.

  Workaround: After converting a switchport with port security to a promiscuous port, apply the port security interface command again. (CSCeg41424)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- If you configure a SPAN session and then apply a SPAN ACL filter to the session, the packets that should be dropped according to the ACL definition are still sent out the SPAN destination port.

  For example, the intent of the following command sequence is to drop packets with source or destination IP address 20.4.1.2 on the SPAN destination port Gigabit Ethernet 6/5:

  ```
  Switch(config)# access-list 1 deny 20.4.1.2
  Switch(config)# monitor session 1 source interface gi6/5
  Switch(config)# monitor session 1 destination interface gi6/7
  Switch(config)# monitor session 1 filter ip access-group 1
  ```

  However, if this is the first time you are applying the ACL filter to the SPAN session, the packets with IP address 20.4.1.2 are still copied to the SPAN destination port.

  If this sample configuration is contained in the startup-config, then the ACL filter would work properly after the Catalyst 4500 series switch boots.

  This caveat only impacts Cisco IOS Release 12.2(25)EWA.

  Workaround: Remove the ACL filter and then re-apply it using the following command sequence:

  ```
  Switch(config)# no monitor session 1 filter ip access-group 1
  Switch(config)# monitor session 1 filter ip access-group 1
  ```

  (CSCsa64231)

- Issuing the **no ip flow ingress** command will not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command.

  (CSCsa67042)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers. (CSCsa57218)

- Modifying a policer may not work if you configure more than 800 policers.

  Workaround: Remove, reconfigure and reinstall policers, or, use less than 800 policers. (CSCsa66422)

- When you use the **vlan** command in interface range configuration mode to configure a range of VLANs on Layer 3 ports, the VLANs might not be created, as in the following example. Additional VLANs will not be created on the Catalyst 4500 series switch until the switch has been reloaded.

  ```
  Switch(config)# int range gi3/3 - 28
  Switch(config-if-range)# sw
  Switch(config-if-range)# no sw
  ```

```
Switch(config-if-range)# vlan 1000-4094
% Command failed on interface GigabitEthernet3/4. Aborting
Switch(config)#
```

Workaround: Create the VLANs in global or interface command mode. CSCsa54831)

- Deleting the trusted boundary configuration from a port that does not have a phone attached to it and which was configured using the **auto qos voip cisco** command leaves the port in an untrusted state. The **auto qos voip cisco** command will configure two CLI's on a port: **qos trust cos** and **qos trust device cisco-phone**. Removing the **qos trust device cisco-phone** command (using the **no qos trust cisco-phone** command) will cause the port to remain in an untrusted state.

  Workaround: None. (CSCsa64726)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA1

This section lists the resolved caveats in Release 12.2(25)EWA1:

- NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

```
cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType                1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot                1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive              1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges       1.3.6.1.4.1.9.9.99999.1.3.4.1.6
```

  (CSCsa81379)

- Cisco Internetwork Operating System (IOS®) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050729-ipv6 (CSCef68324)

Open Caveats in Cisco IOS Release 12.2(25)EWA

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This activity can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

```
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- After a supervisor engine switchover in SSO mode, the Diagnostic Optical Monitoring feature (CLI and MIB support) might not work as expected. The **show interfaces transceiver** command will not display any output.

  Workaround: Reload the supervisor engines. (CSCef67309)

- After moving to a non-redundant chassis, a supervisor engine that was previously configured in SSO mode will not be able to configure router ports or port-channel.

  Workarounds:

  1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR.

  2. Enter the **write memory** command and reload the switch from the non-redundancy chassis. (CSCef67677)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   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)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsa44632)

- If the switch receives an unlearned source MAC address after a security violation, memory is consumed in creating a security violation-related SNMP trap for each source MAC address. If the switch receives several unlearned source MAC addresses at a very high rate, considerable memory is consumed to ensure that the SNMP traps are generated and sent out correctly.

  Workaround: Configure the trap-rate to limit very small number of traps every second. The following configuration sets a trap-rate of 1/2 trap per second (CSCeg41478):

```
Switch(config)#snmp-ser enable traps port-se trap-rate 1
Switch(config)#snmp-ser enable traps port-se trap-rate 2
```

- Under certain rare scenarios, the packet match counter in **show policy-map interface fa6/1** does not show the packets being matched, as in the following configuration:

```
 clearwater#sh policy-map int
  FastEthernet6/2

   Service-policy output: p4

     Class-map: ipc2 (match-all)
       0 packets<---------- It shouldn't stay at '0'.
       Match: access-group name ipacl_2
       police: Per-interface
         Conform: 22937970 bytes Exceed: 977688712 bytes <--- traffic going thru


     Class-map: class-default (match-any)
       410 packets
       Match: any
         410 packets
```

  Workaround: Either enter a shutdown/no shutdown on the port or detach and reapply the service policy. (CSCef30883)

- When a switchport configured with port security is converted from an access to a promiscuous port, the port security configuration is lost. The **show interface** command will show that port security is no longer configured.

  Workaround: After converting a switchport with port security to a promiscuous port, apply the port security interface command again. (CSCeg41424)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- If you configure a SPAN session and then apply a SPAN ACL filter to the session, the packets that should be dropped according to the ACL definition are still sent out the SPAN destination port.

  For example, the intent of the following command sequence is to drop packets with source or destination IP address 20.4.1.2 on the SPAN destination port Gigabit Ethernet 6/5:

```
Switch(config)# access-list 1 deny 20.4.1.2
Switch(config)# monitor session 1 source interface gi6/5
Switch(config)# monitor session 1 destination interface gi6/7
Switch(config)# monitor session 1 filter ip access-group 1
```

  However, if this is the first time you are applying the ACL filter to the SPAN session, the packets with IP address 20.4.1.2 are still copied to the SPAN destination port.

If this sample configuration is contained in the startup-config, then the ACL filter would work properly after the Catalyst 4500 series switch boots.

This caveat only impacts Cisco IOS Release 12.2(25)EWA.

Workaround: Remove the ACL filter and then re-apply it using the following command sequence:

```
Switch(config)# no monitor session 1 filter ip access-group 1
Switch(config)# monitor session 1 filter ip access-group 1
```

(CSCsa64231)

- Issuing the **no ip flow ingress** command will not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command.

  (CSCsa67042)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers. (CSCsa57218)

- Modifying a policer may not work if you configure more than 800 policers.

  Workaround: Remove, reconfigure and reinstall policers, or, use less than 800 policers. (CSCsa66422)

- When you use the **vlan** command in interface range configuration mode to configure a range of VLANs on Layer 3 ports, the VLANs might not be created, as in the following example. Additional VLANs will not be created on the Catalyst 4500 series switch until the switch has been reloaded.

```
Switch(config)# int range gi3/3 - 28
Switch(config-if-range)# sw
Switch(config-if-range)# no sw
Switch(config-if-range)# vlan 1000-4094
% Command failed on interface GigabitEthernet3/4. Aborting
Switch(config)#
```

  Workaround: Create the VLANs in global or interface command mode. CSCsa54831)

- Deleting the trusted boundary configuration from a port that does not have a phone attached to it and which was configured using the **auto qos voip cisco** command leaves the port in an untrusted state. The **auto qos voip cisco** command will configure two CLI's on a port: **qos trust cos** and **qos trust device cisco-phone**. Removing the **qos trust device cisco-phone** command (using the **no qos trust cisco-phone** command) will cause the port to remain in an untrusted state.

  Workaround: None. (CSCsa64726)

- The policers configured on VLANs associated with the trunk ports of a Catalyst 4500 series switch may stop functioning when more than 1000 VLANs have policers applied to them and VLANs are added or deleted from the policer list. For example, if a trunk port allows 1020 VLANs with a policer applied to all VLANs, removing and adding some VLANs from the VLAN list may stop the policers from functioning on any of the VLANs.

  Workaround: If you configure more than 1000 VLANs with policers, remove the excess VLAN policers, disable, and enable QoS globally to restore QoS. For a VLAN list of roughly 1000 VLANs, disable, then enable QoS globally to restore QoS after the VLAN changes are made. (CSCsa57218)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA

This section lists the resolved caveats in Release 12.2(25)EWA:

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)
- When the access VLAN of an access port is converted into an RSPAN VLAN, the **show interface** and **show interface inactive** commands indicate that the interface is up and connected. This problem is strictly cosmetic; the interface is no longer forwarding traffic.

  Workaround: None. (CSCsa44090)
- When a Catalyst 4500 series switch exhausts the packet buffers and can no longer receive packets, the Rx-No_pkt_Buff field in the output of the **show platform interface all** command may not get updated.

  Workaround: None. (CSCef72691)
- Per-flow Border Gateway Protocol (BGP) AS information is not collected. As a result, BGP AS information will not be available in any of the aggregation caches.

  Workaround: None. (CSCin85662)
- Multicast over Generic Routing Encapsulation (GRE) does not work.

  Workaround: None (CSCin85525)
- The PoE status LED on the WS-X4506-GB-T linecard is always off. Moreover, PoE status does not appear in the output of the show environment command.

  Workaround: None. (CSCeh26976)

Open Caveats in Cisco IOS Release 12.2(25)EW

This section lists the open caveats in Cisco IOS Release 12.2(25)EW.

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)
- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then reenable QoS with the **qos global** command. (CSCee52449)
- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This behavior can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)
- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is

disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- After a supervisor engine switchover in SSO mode, the Diagnostic Optical Monitoring feature (CLI and MIB support) might not work as expected. The **show interfaces transceiver** command will not display any output.

  Workaround: Reload the supervisor engines. (CSCef67309)

- After moving to a non-redundant chassis, a supervisor engine that was previously configured in SSO mode will not be able to configure router ports or port-channel.

  Workarounds:

  1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR.

  2. Enter the **write memory** command and reload the switch from the non-redundancy chassis. (CSCef67677)

- When the access VLAN of an access port is converted into an RSPAN VLAN, the **show interface** and **show interface inactive** commands indicate that the interface is up and connected. This problem is strictly cosmetic; the interface is no longer forwarding traffic.

  Workaround: None. (CSCsa44090)

- When a Catalyst 4500 series switch exhausts the packet buffers and can no longer receive packets, the Rx-No_pkt_Buff field in the output of the **show platform interface all** command may not get updated.

  Workaround: None. (CSCef72691)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- Per-flow Border Gateway Protocol (BGP) AS information is not collected. As a result, BGP AS information will not be available in any of the aggregation caches.

  Workaround: None. (CSCin85662)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   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)

- Multicast over Generic Routing Encapsulation (GRE) does not work.

  Workaround: None (CSCin85525)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsa44632)

- If the switch receives an unlearned source MAC address after a security violation, memory is consumed in creating a security violation-related SNMP trap for each source MAC address. If the switch receives several unlearned source MAC addresses at a very high rate, considerable memory is consumed to ensure that the SNMP traps are generated and sent out correctly.

  Workaround: Configure the trap-rate to limit very small number of traps every second. The following configuration sets a trap-rate of 1/2 trap per second (CSCeg41478):

  ```
  Switch(config)#snmp-ser enable traps port-se trap-rate 1
  Switch(config)#snmp-ser enable traps port-se trap-rate 2
  ```

- Under certain rare scenarios, the packet match counter in **show policy-map interface fa6/1** does not show the packets being matched, as in the following configuration:

  ```
  clearwater#sh policy-map int
   FastEthernet6/2

    Service-policy output: p4

      Class-map: ipc2 (match-all)
        0 packets<---------- It shouldn't stay at '0'.
        Match: access-group name ipacl_2
        police: Per-interface
          Conform: 22937970 bytes Exceed: 977688712 bytes <--- traffic going thru


      Class-map: class-default (match-any)
        410 packets
        Match: any
          410 packets
  ```

  Workaround: Either enter a shutdown/no shutdown on the port or detach and reapply the service policy. (CSCef30883)

- When a switchport configured with port security is converted from an access to a promiscuous port, the port security configuration is lost. The **show interface** command will show that port security is no longer configured.

  Workaround: After converting a switchport with port security to a promiscuous port, apply the port security interface command again. (CSCeg41424)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- The PoE status LED on the WS-X4506-GB-T linecard is always off. Moreover, PoE status does not appear in the output of the show environment command.

  Workaround: None. This was fixed in Cisco IOS Release 12.2(25)EWA. (CSCeh26976)

Resolved Caveats in Cisco IOS Release 12.2(25)EW

This section lists the resolved caveats in Release 12.2(25)EW:

- Under conditions where switch communication with the RADIUS server is broken or delayed, 802.1X may either cause the switch to crash or generate memory corruption tracebacks. This issue impacts Releases 12.1(20)EW, 12.2(18)EW, 12.2(18)EW1, 12.2(20)EW and 12.2(20)EWA.

  Workaround: None. (CSCef46146)

- When the gigabit port of a Catalyst 3550 switch with inline power (WS-C3550-25-PWR) is connected to the gigabit port of a Catalyst 4500 series switch with Supervisor Engine WS-X4516 and Release 12.2(18)EW or 12.2(20)EW, the gigabit uplink port on the Catalyst 3550 switch fails POST (lost loopback packet) during bootup.

  Workarounds:

  1. Disconnect the cable connecting the uplink ports on the Catalyst 3550 switch to the Catalyst 4500 series switch before booting the Catalyst 3550 switch. After the Catalyst 3550 switch boots, reconnect the cable.

  2. Shutdown the gigaports on the Catalyst 4500 series switch before booting the Catalyst 3550 switch. After the Catalyst 3550 switch boots, enter a **no shutdown** command on the gigaports of the Catalyst 4500 series switch. (CSC50578)

- Upon power-cycle, a Catalyst 4500 series switch with redundant supervisor engines and Release 12.2(20)EWA may indicate that all modules are faulty.

  Workaround: Enter the **redundancy reload peer** command to reload the standby supervisor engine. Then, reset all the faulty line-cards with the **hw-module slot reset** command. (CSCsa44721)

- Cisco Internetwork Operating System (IOS®) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050729-ipv6 (CSCef68324)

Open Caveats in Cisco IOS Release 12.2(20)EWA4

This section lists the open caveats in Cisco IOS Release 12.2(20)EWA4:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then reenable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This behavior can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is

disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- After a supervisor engine switchover in SSO mode, the Diagnostic Optical Monitoring feature (CLI and MIB support) might not work as expected. The **show interfaces transceiver** command will not display any output.

  Workaround: Reload the supervisor engines. (CSCef67309)

- After moving to a non-redundant chassis, a supervisor engine that was previously configured in SSO mode will not be able to configure router ports or port-channel.

  Workarounds:

  1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR mode.

  2. If you do not perform the first workaround, enter the **write memory** command, and reload the switch from the non-redundancy chassis. (CSCef67677)

- The PoE status LED on the WS-X4506-GB-T linecard is always off. Moreover, PoE status does not appear in the output of the show environment command.

  Workaround: None. This was fixed in Cisco IOS Release 12.2(25)EWA. (CSCeh26976)

Resolved Caveats in Cisco IOS Release 12.2(20)EWA4

This section lists the resolved caveats in Release 12.2(20)EWA4:

- Some (or all) CDP neighbors are invisible.

  It only happens on releases that include the fix for CSCse85200.

  When turning on "debug cdp even," the following message appears:

  ```
  CDP-EV: Received item (type : 9) with invalid length 4
  ```

  Workaround: None. (CSCsf07847)

- Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  (CSCek26492)

- Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

  This vulnerability was discovered during internal testing.

  (CSCec71950)

Open Caveats in Cisco IOS Release 12.2(20)EWA3

This section lists the open caveats in Cisco IOS Release 12.2(20)EWA3:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then reenable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This behavior can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- After a supervisor engine switchover in SSO mode, the Diagnostic Optical Monitoring feature (CLI and MIB support) might not work as expected. The **show interfaces transceiver** command will not display any output.

  Workaround: Reload the supervisor engines. (CSCef67309)
- After moving to a non-redundant chassis, a supervisor engine that was previously configured in SSO mode will not be able to configure router ports or port-channel.

  Workarounds:

  1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR mode.

  2. If you do not perform the first workaround, enter the **write memory** command, and reload the switch from the non-redundancy chassis. (CSCef67677)
- The PoE status LED on the WS-X4506-GB-T linecard is always off. Moreover, PoE status does not appear in the output of the show environment command.

  Workaround: None. This was fixed in Cisco IOS Release 12.2(25)EWA. (CSCeh26976)

Resolved Caveats in Cisco IOS Release 12.2(20)EWA3

This section lists the resolved caveats in Release 12.2(20)EWA3:

- Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability. (CSCei76358)

Open Caveats in Cisco IOS Release 12.2(20)EWA2

This section lists the open caveats in Cisco IOS Release 12.2(20)EWA2:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)
- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then reenable QoS with the **qos global** command. (CSCee52449)
- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This behavior can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)
- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is

disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- After a supervisor engine switchover in SSO mode, the Diagnostic Optical Monitoring feature (CLI and MIB support) might not work as expected. The **show interfaces transceiver** command will not display any output.

  Workaround: Reload the supervisor engines. (CSCef67309)

- After moving to a non-redundant chassis, a supervisor engine that was previously configured in SSO mode will not be able to configure router ports or port-channel.

  Workarounds:

  1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR mode.

  2. If you do not perform the first workaround, enter the **write memory** command, and reload the switch from the non-redundancy chassis. (CSCef67677)

- The PoE status LED on the WS-X4506-GB-T linecard is always off. Moreover, PoE status does not appear in the output of the show environment command.

  Workaround: None. This was fixed in Cisco IOS Release 12.2(25)EWA. (CSCeh26976)

Resolved Caveats in Cisco IOS Release 12.2(20)EWA2

This section lists the resolved caveats in Release 12.2(20)EWA2:

- Cisco Internetwork Operating System (IOS®) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050729-ipv6 (CSCef68324)

Open Caveats in Cisco IOS Release 12.2(20)EWA1

This section lists the open caveats in Cisco IOS Release 12.2(20)EWA1:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then reenable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This behavior can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- After a supervisor engine switchover in SSO mode, the Diagnostic Optical Monitoring feature (CLI and MIB support) might not work as expected. The **show interfaces transceiver** command will not display any output.

  Workaround: Reload the supervisor engines. (CSCef67309)

- After moving to a non-redundant chassis, a supervisor engine that was previously configured in SSO mode will not be able to configure router ports or port-channel.

  Workarounds:

  1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR mode.

  2. If you do not perform the first workaround, enter the **write memory** command, and reload the switch from the non-redundancy chassis. (CSCef67677)

- The PoE status LED on the WS-X4506-GB-T linecard is always off. Moreover, PoE status does not appear in the output of the show environment command.

  Workaround: None. This was fixed in Cisco IOS Release 12.2(25)EWA. (CSCeh26976)

Resolved Caveats in Cisco IOS Release 12.2(20)EWA1

This section lists the resolved caveats in Release 12.2(20)EWA1:

- NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

  ```
  cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
  cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
  cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
  cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
  cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
  cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
  cnfFeatureType                1.3.6.1.4.1.9.9.99999.1.3.4.1.1
  cnfFeatureSlot                1.3.6.1.4.1.9.9.99999.1.3.4.1.2
  cnfFeatureActive              1.3.6.1.4.1.9.9.99999.1.3.4.1.3
  cnfFeatureAttaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.4
  cnfFeatureDetaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.5
  cnfFeatureConfigChanges       1.3.6.1.4.1.9.9.99999.1.3.4.1.6
  ```

  (CSCsa81379)

Open Caveats in Cisco IOS Release 12.2(20)EWA

This section lists the open caveats in Cisco IOS Release 12.2(20)EWA.

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then reenable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This behavior can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is

disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- After a supervisor engine switchover in SSO mode, the Diagnostic Optical Monitoring feature (CLI and MIB support) might not work as expected. The **show interfaces transceiver** command will not display any output.

  Workaround: Reload the supervisor engines. (CSCef67309)

- After moving to a non-redundant chassis, a supervisor engine that was previously configured in SSO mode will not be able to configure router ports or port-channel.

  Workarounds:

  1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR mode.

  2. If you do not perform the first workaround, enter the **write memory** command, and reload the switch from the non-redundancy chassis. (CSCef67677)

- The PoE status LED on the WS-X4506-GB-T linecard is always off. Moreover, PoE status does not appear in the output of the show environment command.

  Workaround: None. This was fixed in Cisco IOS Release 12.2(25)EWA. (CSCeh26976)

Resolved Caveats in Cisco IOS Release 12.2(20)EWA

This section lists the resolved caveats in Release 12.2(20)EWA:

- The DHCP snooping database agent has a maximum of 8192 entries. If the number of DHCP bindings learned by the system exceeds this number, the entries in the database agent will be cleared out, the entries in hardware will be retained, and switching will continue. However, upon reload, bindings and connectivity will be lost.

  Workaround: None. (CSCee34375)

- If IP source guard and QoS policies with large ACLs are configured on an interface, deleting the QoS policy will not clear the policers from the hardware.

  Workaround: Either remove the IP source guard configuration using the **no ip verify source vlan dhcp-snooping port-security** command and reconfigure using the **ip verify source vlan dhcp-snooping port-security** command or shut down the interface (after removing the policy) using the **shutdown** command, and reactivate it using the **no shutdown** command. (CSCee44402)

- A Catalyst 4500 series switch with a 1000 W power supply might display the following message during bootup sequence and also when you enter the **show idprom power-supply** command:

  ```
  %C4K_SUPERVISOR-3-POWERSUPPLYSEEPROMINVALID: Invalid data in power supply 1's serial
  eeprom
  ```

  This is cosmetic only and does not impact system performance. (CSCee54636)

- When you use private VLANs on the Catalyst 4500 series switch Supervisor Engine V (WS-X4516), old ARP entries will not timeout of the ARP cache without manually clearing the ARP entry. This has no effect on production.

  Workaround: Issue the **clear arp** command on the supervisor engine. (CSCee73094)

Open Caveats in Cisco IOS Release 12.2(20)EW4

This section lists the open caveats in Cisco IOS Release 12.2(20)EW4.

- For Release 12.2(18)EW or later, when the Gigabit Ethernet port of a Catalyst 3550 switch with inline power (WS-C3550-25-PWR) is connected to the Gigabit Ethernet port of a Catalyst 4500 series switch with a Supervisor Engine V (WS-X4516), the port on the Catalyst 3500 switch fails POST (power-on self test) during startup.

  Workarounds:

  1. Before starting up the Catalyst 3550 switch, disconnect the cable connecting the uplink ports on the Catalyst 3550 switch to the Catalyst 4500 series switch. Once the Catalyst 3550 switch boots, reconnect the cable.

  2. Before starting up the Catalyst 3550 switch, issue the **shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 series switch. After starting up the Catalyst 3550 switch, issue the **no shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 switch. (CSCee50578)

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- The DHCP snooping database agent has a maximum of 8192 entries. If the number of DHCP bindings learned by the system exceeds this number, the entries in the database agent will be cleared out, the entries in hardware will be retained, and switching will continue. However, upon reload, bindings and connectivity will be lost.

  Workaround: None. (CSCee34375)

- If IP source guard and QoS policies with large ACLs are configured on an interface, deleting the QoS policy will not clear the policers from the hardware.

  Workaround: Either remove the IP source guard configuration using the **no ip verify source vlan dhcp-snooping port-security** command and reconfigure using **ip verify source vlan dhcp-snooping port-security** command or shut down the interface (after removing the policy) using the **shutdown** command and reactivate it using the **no shutdown** command. (CSCee44402)

- On a system reload, some of the QoS policies that had previously loaded into the hardware, may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, then reenable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This behavior can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting flapping of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

Resolved Caveats in Cisco IOS Release 12.2(20)EW4

This section lists the resolved caveats in release 12.2(20)EW4:

- Some (or all) CDP neighbors are invisible.

  It only happens on releases that include the fix for CSCse85200.

  When turning on "debug cdp even," the following message appears:

  ```
  CDP-EV: Received item (type : 9) with invalid length 4
  ```

  Workaround: None. (CSCsf07847)

- Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  (CSCek26492)

- CSCec71950

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

  This vulnerability was discovered during internal testing.

Open Caveats in Cisco IOS Release 12.2(20)EW3

This section lists the open caveats in Cisco IOS Release 12.2(20)EW3.

- For Release 12.2(18)EW or later, when the Gigabit Ethernet port of a Catalyst 3550 switch with inline power (WS-C3550-25-PWR) is connected to the Gigabit Ethernet port of a Catalyst 4500 series switch with a Supervisor Engine V (WS-X4516), the port on the Catalyst 3500 switch fails POST (power-on self test) during startup.

  Workarounds:

  1. Before starting up the Catalyst 3550 switch, disconnect the cable connecting the uplink ports on the Catalyst 3550 switch to the Catalyst 4500 series switch. Once the Catalyst 3550 switch boots, reconnect the cable.

  2. Before starting up the Catalyst 3550 switch, issue the **shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 series switch. After starting up the Catalyst 3550 switch, issue the **no shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 switch. (CSCee50578)

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- The DHCP snooping database agent has a maximum of 8192 entries. If the number of DHCP bindings learned by the system exceeds this number, the entries in the database agent will be cleared out, the entries in hardware will be retained, and switching will continue. However, upon reload, bindings and connectivity will be lost.

  Workaround: None. (CSCee34375)

- If IP source guard and QoS policies with large ACLs are configured on an interface, deleting the QoS policy will not clear the policers from the hardware.

  Workaround: Either remove the IP source guard configuration using the **no ip verify source vlan dhcp-snooping port-security** command and reconfigure using **ip verify source vlan dhcp-snooping port-security** command or shut down the interface (after removing the policy) using the **shutdown** command and reactivate it using the **no shutdown** command. (CSCee44402)

- On a system reload, some of the QoS policies that had previously loaded into the hardware, may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, then reenable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This behavior can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting flapping of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

Resolved Caveats in Cisco IOS Release 12.2(20)EW3

This section lists the resolved caveats in release 12.2(20)EW3:

- Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability. (CSCei76358)
- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  (CSCei61732)

Open Caveats in Cisco IOS Release 12.2(20)EW2

This section lists the open caveats in Cisco IOS Release 12.2(20)EW2.

- For Release 12.2(18)EW or later, when the Gigabit Ethernet port of a Catalyst 3550 switch with inline power (WS-C3550-25-PWR) is connected to the Gigabit Ethernet port of a Catalyst 4500 series switch with a Supervisor Engine V (WS-X4516), the port on the Catalyst 3500 switch fails POST (power-on self test) during startup.

  Workarounds:

  1. Before starting up the Catalyst 3550 switch, disconnect the cable connecting the uplink ports on the Catalyst 3550 switch to the Catalyst 4500 series switch. Once the Catalyst 3550 switch boots, reconnect the cable.

  2. Before starting up the Catalyst 3550 switch, issue the **shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 series switch. After starting up the Catalyst 3550 switch, issue the **no shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 switch. (CSCee50578)
- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)
- The DHCP snooping database agent has a maximum of 8192 entries. If the number of DHCP bindings learned by the system exceeds this number, the entries in the database agent will be cleared out, the entries in hardware will be retained, and switching will continue. However, upon reload, bindings and connectivity will be lost.

  Workaround: None. (CSCee34375)
- If IP source guard and QoS policies with large ACLs are configured on an interface, deleting the QoS policy will not clear the policers from the hardware.

  Workaround: Either remove the IP source guard configuration using the **no ip verify source vlan dhcp-snooping port-security** command and reconfigure using **ip verify source vlan dhcp-snooping port-security** command or shut down the interface (after removing the policy) using the **shutdown** command and reactivate it using the **no shutdown** command. (CSCee44402)
- On a system reload, some of the QoS policies that had previously loaded into the hardware, may fail to load due to limited space.

Workaround: Disable QoS with the **no qos** command, then reenable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This behavior can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting flapping of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

Resolved Caveats in Cisco IOS Release 12.2(20)EW2

This section lists the resolved caveats in release 12.2(20)EW2:

- Cisco Internetwork Operating System (IOS®) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050729-ipv6 (CSCef68324)

Open Caveats in Cisco IOS Release 12.2(20)EW1

This section lists the open caveats in Cisco IOS Release 12.2(20)EW1.

- For Release 12.2(18)EW or later, when the Gigabit Ethernet port of a Catalyst 3550 switch with inline power (WS-C3550-25-PWR) is connected to the Gigabit Ethernet port of a Catalyst 4500 series switch with a Supervisor Engine V (WS-X4516), the port on the Catalyst 3500 switch fails POST (power-on self test) during startup.

  Workarounds:

  1. Before starting up the Catalyst 3550 switch, disconnect the cable connecting the uplink ports on the Catalyst 3550 switch to the Catalyst 4500 series switch. Once the Catalyst 3550 switch boots, reconnect the cable.

  2. Before starting up the Catalyst 3550 switch, issue the **shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 series switch. After starting up the Catalyst 3550 switch, issue the **no shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 switch. (CSCee50578)

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- The DHCP snooping database agent has a maximum of 8192 entries. If the number of DHCP bindings learned by the system exceeds this number, the entries in the database agent will be cleared out, the entries in hardware will be retained, and switching will continue. However, upon reload, bindings and connectivity will be lost.

  Workaround: None. (CSCee34375)

- If IP source guard and QoS policies with large ACLs are configured on an interface, deleting the QoS policy will not clear the policers from the hardware.

  Workaround: Either remove the IP source guard configuration using the **no ip verify source vlan dhcp-snooping port-security** command and reconfigure using **ip verify source vlan dhcp-snooping port-security** command or shut down the interface (after removing the policy) using the **shutdown** command and reactivate it using the **no shutdown** command. (CSCee44402)

- On a system reload, some of the QoS policies that had previously loaded into the hardware, may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, then reenable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This behavior can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is

disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting flapping of the link.

Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

Resolved Caveats in Cisco IOS Release 12.2(20)EW1

This section lists the resolved caveats in release 12.2(20)EW1:

- NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supersedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

  ```
  cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
  cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
  cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
  cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
  cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
  cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
  cnfFeatureType                1.3.6.1.4.1.9.9.99999.1.3.4.1.1
  cnfFeatureSlot                1.3.6.1.4.1.9.9.99999.1.3.4.1.2
  cnfFeatureActive              1.3.6.1.4.1.9.9.99999.1.3.4.1.3
  cnfFeatureAttaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.4
  cnfFeatureDetaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.5
  cnfFeatureConfigChanges       1.3.6.1.4.1.9.9.99999.1.3.4.1.6
  ```

  (CSCsa81379)

Open Caveats in Cisco IOS Release 12.2(20)EW

This section lists the open caveats in Cisco IOS Release 12.2(20)EW.

- For Release 12.2(18)EW or later, when the Gigabit Ethernet port of a Catalyst 3550 switch with inline power (WS-C3550-25-PWR) is connected to the Gigabit Ethernet port of a Catalyst 4500 series switch with a Supervisor Engine V (WS-X4516), the port on the Catalyst 3500 switch fails POST (power-on self test) during startup.

  Workarounds:

  1. Before starting up the Catalyst 3550 switch, disconnect the cable connecting the uplink ports on the Catalyst 3550 switch to the Catalyst 4500 series switch. Once the Catalyst 3550 switch boots, reconnect the cable.

  2. Before starting up the Catalyst 3550 switch, issue the **shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 series switch. After starting up the Catalyst 3550 switch, issue the **no shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 switch. (CSCee50578)

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- The DHCP snooping database agent has a maximum of 8192 entries. If the number of DHCP bindings learned by the system exceeds this number, the entries in the database agent will be cleared out, the entries in hardware will be retained, and switching will continue. However, upon reload, bindings and connectivity will be lost.

  Workaround: None. (CSCee34375)

- If IP source guard and QoS policies with large ACLs are configured on an interface, deleting the QoS policy will not clear the policers from the hardware.

  Workaround: Either remove the IP source guard configuration using the **no ip verify source vlan dhcp-snooping port-security** command and reconfigure using **ip verify source vlan dhcp-snooping port-security** command or shut down the interface (after removing the policy) using the **shutdown** command and reactivate it using the **no shutdown** command. (CSCee44402)

- On a system reload, some of the QoS policies that had previously loaded into the hardware, may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, then reenable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This behavior can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is

disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting flapping of the link.

Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)
- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)
- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

Resolved Caveats in Cisco IOS Release 12.2(20)EW

This section lists the resolved caveats in release 12.2(20)EW:

- Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may cause a reload upon successful exploitation.

  (CSCed40933)
- When 802.1Q and Layer 2 Protocol Tunneling are disabled on a switch, and the switch is rebooted after saving the configuration, spanning-tree BPDU filtering is not disabled automatically on the port.

  Workaround: Manually disable spanning-tree BPDU filtering on the interface with the **no spanning-tree bpdufilter** command. (CSCec88311)
- When DHCP snooping, IP source guard, and trunks are configured on all 240 interfaces on a Catalyst 4500 series switch equipped with a Supervisor Engine II+, the switch may exhaust its TCAM space.

  Workaround: None. (CSCed18765)
- When Layer 3 fragmentation fails, a Catalyst 4500 series switch that uses Supervisor Engine IV sends back the wrong ICMP code and causes the Path MTU auto-discovery feature to fail. The switch returns the code “ICMP Host unreachable / Communication administratively filtered (code 13)," yet the correct code is "ICMP Host unreachable / Fragmentation needed but DF-Bit set (Code 4)."

  Workaround: None. (CSCed56513)
- When you upgrade a Cisco IOS software image from Release 12.1(12c) or 12.1(19)E to a release in the 12.2 release train, the following syslog message appears:
  "00:00:01: %C4K_IOSSYS-3-BLANKSTARTUPCONFIG: Blank or invalid startup-config, booting up with defaults".

  Workaround: You may ignore the message. (CSCed26025)

- When configured for VRF-Lite, a Catalyst 4500 series switch inadvertently forwards packets received on the VRF interface for those destinations not in the VRF routing table. Instead of dropping the packets, the switch forwards them using the global routing table.

  Workaround: Issue the command **ip route vrf <vrf name> 0.0.0.0 0.0.0.0 null 0** to drop the packet. (CSCed20990)
- The **show mod** command will not display the correct status of a WS-X4604-GWY module if the gateway module has failed. The status of the module incorrectly displays as “Ok,” but the correct status is “Offline.” This problem has been resolved in the Release 12.3(8.3)T image of the WS-X4604-GWY module.

  Workaround: Use SNMP to monitor both the gateway module and the supervisor engine as separate devices. (CSCea90578)
- Ports in suspended mode due to misconfiguration in the LACP port channel do not recover, even after reconfiguring the ports. This situation occurs when most ports are configured for 802.1X encapsulation and one or more ports are not.

  Workaround: Enter the **switchport trunk encap dot1q** command to add the suspended port to the channel, shut down the port using the **shutdown** command, and then enter the **no shutdown** command to force the port to stay active. This action ensures that the port gets added to the port channel. (CSCeb78999)

Open Caveats in Cisco IOS Release 12.2(18)EW7

This section lists the open caveats in Cisco IOS Release 12.2(18)EW7.

- When 802.1Q and Layer 2 Protocol Tunneling are disabled on a switch, and the switch is rebooted after saving the configuration, spanning-tree BPDU filtering is not disabled automatically on the port.

  Workaround: Manually disable spanning-tree BPDU filtering on the interface with the **no spanning-tree bpdufilter** command. (CSCec88311)
- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)
- On a Catalyst 4500 series switch with Gigabit Ethernet Switching Modules, link flaps may occur when you pull out TX cables on a giga ethernet interface configured with "speed nonnegotiate.”

  Workaround: Do not set “speed nonnegotiate.” (CSCeg57297)
- Inserting the WS-X4232-RJ-XX or WS-X4124-FX-M linecards into a Catalyst 4500 series switch running Cisco IOS Release 12.2(18)EW7 causes the switch to reload continuously.

  This problem is not present in Cisco IOS Release 12.2(25)EWA7.

  Workaround: Remove these linecards or upgrade to Cisco IOS Release 12.2(25)EWA7. (CSCsg43414)

Resolved Caveats in Cisco IOS Release 12.2(18)EW7

This section lists the resolved caveats in release 12.2(18)EW7:

- Some (or all) CDP neighbors are invisible.

  It only happens on releases that include the fix for CSCse85200.

When turning on "debug cdp even," the following message appears:

```
CDP-EV: Received item (type : 9) with invalid length 4
```

Workaround: None. (CSCsf07847)

Open Caveats in Cisco IOS Release 12.2(18)EW6

This section lists the open caveats in Cisco IOS Release 12.2(18)EW6.

- When 802.1Q and Layer 2 Protocol Tunneling are disabled on a switch, and the switch is rebooted after saving the configuration, spanning-tree BPDU filtering is not disabled automatically on the port.

  Workaround: Manually disable spanning-tree BPDU filtering on the interface with the **no spanning-tree bpdufilter** command. (CSCec88311)
- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)
- On a Catalyst 4500 series switch with Gigabit Ethernet Switching Modules, link flaps may occur when you pull out TX cables on a giga ethernet interface configured with "speed nonnegotiate.”

  Workaround: Do not set “speed nonnegotiate.” (CSCeg57297)
- Inserting the WS-X4232-RJ-XX or WS-X4124-FX-M linecards into a Catalyst 4500 series switch running Cisco IOS Release 12.2(18)EW6 causes the switch to reload continuously.

  This problem is not present in Cisco IOS Release 12.2(25)EWA7.

  Workaround: Remove these linecards or upgrade to Cisco IOS Release 12.2(25)EWA7. (CSCsg43414)

Resolved Caveats in Cisco IOS Release 12.2(18)EW6

This section lists the resolved caveats in release 12.2(18)EW6:

- Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability. (CSCei76358)
- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  (CSCei61732)
- If a Catalyst 4500 series switch is configured to receive STP packets, a malformed packet sent to the switch on the local LAN may cause the device to reload.

  Workaround: None. (CSCsa96905)
- If ARP Inspection and DHCP Snooping are enabled and MAC ACLs are applied on a Catalyst 4500 series switch, the switch shows high CPU.

  The **show platform health** command shows that the processes holding the CPU are:

  - KxAclPathMan update

  - TagMan-RecreateMtegR
  - K2L2 Address Table R

  Workaround: Remove the MAC ACLs. (CSCsa63528)

- If storm control is configured on an interface and storm control disables the interface, the ARP table does not update its database after you manually perform a link up/down.

  Workaround: Allow storm control to disable and re-enable the interface. (CSCsb49409)

- When a WS-X4148-RJ45V is configured to “auto” (negotiate) and is connected to an Intel Pro 1000 MT NIC card, the link is negotiated to a port speed of 10 and “full” duplex rather than a port speed of 100 and “full” duplex.

  Workaround: None. (CSCsa55172)

- If an RP is also a first hop Router, the first mcast packet is dropped.

  Workaround: Do not use first hop router as an RP or use dense mode. (CSCsc51906)

- When the 15K Sun server is a link partner to WS-X4118 and connected to a blocking port, rebooting the server may cause packets in the input queue of the port to be sent to the supervisor engine as bad packets. If this condition occurs, packets could remain in the input queue even after the port is shutdown. Packets left in the input queue will be forwarded indefinitely to the supervisor engine, causing flooding and high CPU utilization.

  Workarounds:

  1. Reset the line card **hw-module reset**.

  2. Remove and reinsert line card from the chassis.

  (CSCei19499)

- When configuring a monitor session and the learning option is enabled, the learning option is not shown in the stored config, but it shows in the output of the **show monitor** command. The learning option is disabled after reboot.

  Workaround: None. (CSCsb03748)

- A Catalyst 4500 series switch does not forward an 802.1X request with NULL credentials.

  Workaround: None. (CSCej03858)

- If loopguard is enabled on a port, which is participating in spanning tree (and is in BLK state), it may go into loop inconsistent state and stops receiving BPDUs from its neighbor.

  The problem is fixed in Cisco IOS Releases 12.2(18)EW6, 12.2(25)EWA5, and 12.2(31)SG.

  Workarounds:

  1. Issue **shutdown**, then **no shutdown** on the port stuck.

  2. Disable loop guard on the port, then enable it.

  (CSCsc04047)

- A Catalyst 4500 series switch running in pim dense-mode marks the OIL of (*,G) with an "H" flag (hardware switching flag). Ordinarily, switches operating in pim dense-mode should not use (*,G) to forward traffic.

  This situation does not impact (S,G) multicast traffic forwarding.

  Workaround: None. (CSCeh46536)

- After configuring **speed nonnegotiate** in an interface range on a WS-X4306 module on a Catalyst 4500 series switch, Symbol-Err and Sequence-Err counters may increase.

Workaround: Link up these ports with the **no shut** command. (CSCsc71324)

- When 802.1x accounting is enabled, the Framed-IP-Address[8] attribute is not included in accounting messages generated on ports with **ip dhcp snooping trust** enabled.

  Workaround: None. (CSCsb46019)

- When HF is in pim dense mode, after a Catalyst 4500 series switch boots initially, (s,g) mcast traffic arriving on the switch is not forwarded to the intended destination despite a *,g for that group being present on the system.

  Workaround: Run the **clear ip mroute *** command multiple times. (CSCsb50317)

- If the system MTU is not configured to the default MTU value, the interface MTU cannot return to the default value even if it's cleared by the **no MTU** command in interface mode.

  Workaround: Clear the system MTU first, then clear the interface MTU.

- On a Catalyst 4500 series switch, when igmp-snooping static multicast entries are removed from a forwarding table after shutdown/no shutdown sequence on the port-channel interface on neighbor switch, communication may be lost.

  Workarounds:

  1. Use the **mac-address-table static vlan interface** command rather than the **ip igmp snooping vlan static interface** command.

  2. Use the Cisco IOS Release 12.1E Train.

  (CSCsa78002)

- When the RPF changes while the upstream router is still forwarding mcast packers, the (S,G) uptime doesn't count down but gets refreshed by the mcast packets that the Catalyst 4500 series switch is receiving. This situation does not let the switch send PIM prune messages to the upstream router. It causes unwanted mcast packets to flow across links and makes the link congested.

  If either the RPF interface does not change or it changes when the upstream router has pruned the link towards the downstream router, the prune process happens every 3 mins as expected.

  Workaround: Clear ip mroute for that (S,G). (CSCsa74825)

- If a VLAN assigned to a port via RADIUS by 802.1x does not exist on a switch, the switch may crash. This issue impacts Cisco IOS Releases 12.2(18)EW, 12.2(18)EW1, 12.2(18)EW2, 12.2(18)EW3, 12.2(18)EW4, 12.2(25)EWA and 12.2(25)EWA1.

  Workaround: Do not configure RADIUS to assign VLANs that do not exist. (CSCsb20052)

- Symptoms: The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally-exploitable buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error.

  Conditions: The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

  Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759—VTP version field DoS

  - CSCse40078/CSCse47765—Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

  (CSCei54611)

- Symptoms: The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

  Conditions: The packets must be received on a trunk enabled port.

  Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759—VTP version field DoS
  - CSCse40078/CSCse47765—Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

  (CCSCsd34759)

- Symptoms: A router may crash if it receives a packet with a specific crafted IP option

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved

  (CSCek26492)

Open Caveats in Cisco IOS Release 12.2(18)EW5

This section lists the open caveats in Cisco IOS Release 12.2(18)EW5.

- When 802.1Q and Layer 2 Protocol Tunneling are disabled on a switch, and the switch is rebooted after saving the configuration, spanning-tree BPDU filtering is not disabled automatically on the port.

  Workaround: Manually disable spanning-tree BPDU filtering on the interface with the **no spanning-tree bpdufilter** command. (CSCec88311)

- When DHCP snooping, IP source guard, and trunks are configured on all 240 interfaces of a Catalyst 4500 series switch that is equipped with a Supervisor Engine II+, all TCAM space on the switch might be exhausted.

  Workaround: None. (CSCed18765)

- When configured for VRF-Lite, a Catalyst 4500 series switch incorrectly forwards packets received on the VRF interface for those destinations not in the VRF routing table. Instead of dropping the packet, the switch forwards the packet using the global routing table.

  Workaround: Enter the **ip route vrf <vrf name> 0.0.0.0 0.0.0.0 null 0** command. (CSCed20990)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- If power is denied for an interface, the following console message is printed every five seconds:

  %ILPOWER-5-ILPOWER_POWER_DENY: Interface Gi6/29: inline power denied

  Despite this message, the system is functioning properly.

  Workaround: Turn off logging on the console with the **no logging console** command. (CSCed67157)

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

  Workarounds:

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

  2. Configure the media converter to autonegotiate the speed and duplex instead of running at 100 Mbps and full duplex. (CSCee62109)

Resolved Caveats in Cisco IOS Release 12.2(18)EW5

This section lists the resolved caveats in release 12.2(18)EW5:

- Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability. (CSCei76358)
- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  (CSCei61732)

Open Caveats in Cisco IOS Release 12.2(18)EW4

This section lists the open caveats in Cisco IOS Release 12.2(18)EW4.

- When 802.1Q and Layer 2 Protocol Tunneling are disabled on a switch, and the switch is rebooted after saving the configuration, spanning-tree BPDU filtering is not disabled automatically on the port.

  Workaround: Manually disable spanning-tree BPDU filtering on the interface with the **no spanning-tree bpdufilter** command. (CSCec88311)

- When DHCP snooping, IP source guard, and trunks are configured on all 240 interfaces of a Catalyst 4500 series switch that is equipped with a Supervisor Engine II+, all TCAM space on the switch might be exhausted.

  Workaround: None. (CSCed18765)

- When configured for VRF-Lite, a Catalyst 4500 series switch incorrectly forwards packets received on the VRF interface for those destinations not in the VRF routing table. Instead of dropping the packet, the switch forwards the packet using the global routing table.

  Workaround: Enter the **ip route vrf <vrf name> 0.0.0.0 0.0.0.0 null 0** command. (CSCed20990)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)
- If power is denied for an interface, the following console message is printed every five seconds:

  %ILPOWER-5-ILPOWER_POWER_DENY: Interface Gi6/29: inline power denied

  Despite this message, the system is functioning properly.

  Workaround: Turn off logging on the console with the **no logging console** command. (CSCed67157)
- Interfaces on the module WS-X4148-RJ45V may not establish a link with a Daiden DN-2800G media converter, when both the switch and the media converter interfaces are configured to operate at 100 Mbps and full duplex. This situation occurs when the interface on the module is configured to automatically detect and power up devices inline with the **power inline auto** command. This caveat appears in all software releases.

  Workarounds:

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

  2. Configure the media converter to autonegotiate the speed and duplex instead of running at 100 Mbps and full duplex. (CSCee62109)

Resolved Caveats in Cisco IOS Release 12.2(18)EW4

This section lists the resolved caveats in release 12.2(18)EW4:

- NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supersedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

  ```
  cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
  cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
  cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
  cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
  cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
  cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
  cnfFeatureType                1.3.6.1.4.1.9.9.99999.1.3.4.1.1
  cnfFeatureSlot                1.3.6.1.4.1.9.9.99999.1.3.4.1.2
  cnfFeatureActive              1.3.6.1.4.1.9.9.99999.1.3.4.1.3
  cnfFeatureAttaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.4
  cnfFeatureDetaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.5
  cnfFeatureConfigChanges       1.3.6.1.4.1.9.9.99999.1.3.4.1.6
  ```

  (CSCsa81379)

Open Caveats in Cisco IOS Release 12.2(18)EW3

This section lists the open caveats in Cisco IOS Release 12.2(18)EW3.

- When 802.1Q and Layer 2 Protocol Tunneling are disabled on a switch, and the switch is rebooted after saving the configuration, spanning-tree BPDU filtering is not disabled automatically on the port.

  Workaround: Manually disable spanning-tree BPDU filtering on the interface with the **no spanning-tree bpdufilter** command. (CSCec88311)

- When DHCP snooping, IP source guard, and trunks are configured on all 240 interfaces of a Catalyst 4500 series switch that is equipped with a Supervisor Engine II+, all TCAM space on the switch might be exhausted.

  Workaround: None. (CSCed18765)

- When configured for VRF-Lite, a Catalyst 4500 series switch incorrectly forwards packets received on the VRF interface for those destinations not in the VRF routing table. Instead of dropping the packet, the switch forwards the packet using the global routing table.

  Workaround: Enter the **ip route vrf <vrf name> 0.0.0.0 0.0.0.0 null 0** command. (CSCed20990)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- If power is denied for an interface, the following console message is printed every five seconds:

  %ILPOWER-5-ILPOWER_POWER_DENY: Interface Gi6/29: inline power denied

  Despite this message, the system is functioning properly.

  Workaround: Turn off logging on the console with the **no logging console** command. (CSCed67157)

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

  Workarounds:

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

  2. Configure the media converter to autonegotiate the speed and duplex instead of running at 100 Mbps and full duplex. (CSCee62109)

Resolved Caveats in Cisco IOS Release 12.2(18)EW3

This section lists the resolved caveats in release 12.2(18)EW3:

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP "hard" error messages
2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP "source quench" messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. (CSCef60659)

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. (CSCef44699)

- Ports in suspended mode due to misconfiguration in the LACP port channel do not recover, even after reconfiguring the ports. This situation occurs when most ports are configured for dot1q encapsulation and one or more ports are not.

  Workaround: Enter the **switchport trunk encap dot1q** command to add the suspended port to the channel, shut down the port using the **shutdown** command, and then enter the **no shutdown** command to force the port to stay active. This action ensures that the port gets added to the port channel. (CSCeb78999)

- CSCec71950

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent

Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

Cisco has made free software available to address this vulnerability for affected customers.

There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability was discovered during internal testing.

Open Caveats in Cisco IOS Release 12.2(18)EW2

This section lists the open caveats in Cisco IOS Release 12.2(18)EW2.

- When 802.1Q and Layer 2 Protocol Tunneling are disabled on a switch, and the switch is rebooted after saving the configuration, spanning-tree BPDU filtering is not disabled automatically on the port.

  Workaround: Manually disable spanning-tree BPDU filtering on the interface with the **no spanning-tree bpdufilter** command. (CSCec88311)
- When DHCP snooping, IP source guard, and trunks are configured on all 240 interfaces of a Catalyst 4500 series switch that is equipped with a Supervisor Engine II+, all TCAM space on the switch might be exhausted.

  Workaround: None. (CSCed18765)
- When configured for VRF-Lite, a Catalyst 4500 series switch incorrectly forwards packets received on the VRF interface for those destinations not in the VRF routing table. Instead of dropping the packet, the switch forwards the packet using the global routing table.

  Workaround: Enter the **ip route vrf <vrf name> 0.0.0.0 0.0.0.0 null 0** command. (CSCed20990)
- Ports in suspended mode due to misconfiguration in the LACP port channel do not recover, even after reconfiguring the ports. This situation occurs when most ports are configured for dot1q encapsulation and one or more ports are not.

  Workaround: Enter the **switchport trunk encap dot1q** command to add the suspended port to the channel, shut down the port using the **shutdown** command, and then enter the **no shutdown** command to force the port to stay active. This action ensures that the port gets added to the port channel. (CSCeb78999)
- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)
- If power is denied for an interface, the following console message is printed every five seconds:

  %ILPOWER-5-ILPOWER_POWER_DENY: Interface Gi6/29: inline power denied

  Despite this message, the system is functioning properly.

  Workaround: Turn off logging on the console with the **no logging console** command. (CSCed67157)
- Interfaces on the module WS-X4148-RJ45V may not establish a link with a Daiden DN-2800G media converter, when both the switch and the media converter interfaces are configured to operate at 100 Mbps and full duplex. This situation occurs when the interface on the module is configured to automatically detect and power up devices inline with the **power inline auto** command. This caveat appears in all software releases.

Workarounds:

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

2. Configure the media converter to autonegotiate the speed and duplex instead of running at 100 Mbps and full duplex. (CSCee62109)

Resolved Caveats in Cisco IOS Release 12.2(18)EW2

This section lists the resolved caveats in release 12.2(18)EW2:

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. (CSCed78149)

- Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can cause a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)
  (CSCed65285)

- Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can cause a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In UserService (RADIUS) is not affected by these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)
(CSCed65778)

- A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command 'bgp log-neighbor-changes' configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  If a misformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

  Cisco has made free software available to address this problem.

  (CSCee67450)

- Cisco IOS® devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID CSCee50294.

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays up regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into err-disable mode because of the continuous flapping of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV running Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine running Release 12.1(19)EW (or later). (CSCeb36355)

- For Release 12.2(18)EW or later, when the Gigabit Ethernet port of a Catalyst 3550 switch with inline power (WS-C3550-25-PWR) is connected to the Gigabit Ethernet port of a Catalyst 4500 series switch with a Supervisor Engine V (WS-X4516), the port on the Catalyst 3500 switch fails POST (power-on self test) during startup.

Workarounds:

1. Before starting up the Catalyst 3550 switch, disconnect the cable connecting the uplink ports on the Catalyst 3550 switch to the Catalyst 4500 series switch. Once the Catalyst 3550 switch boots, reconnect the cable.

2. Before starting up the Catalyst 3550 switch, enter the **shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 series switch. After starting up the Catalyst 3550 switch, enter the **no shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 switch. (CSCee50578)

Open Caveats in Cisco IOS Release 12.2(18)EW1

This section lists the open caveats in Cisco IOS Release 12.2(18)EW1.

- When 802.1Q and Layer 2 Protocol Tunneling are disabled on a switch, and the switch is rebooted after saving the configuration, spanning-tree BPDU filtering is not disabled automatically on the port.

  Workaround: Manually disable spanning-tree BPDU filtering on the interface with the **no spanning-tree bpdufilter** command. (CSCec88311)

- When DHCP snooping, IP source guard, and trunks are configured on all 240 interfaces of a Catalyst 4500 series switch that is equipped with a Supervisor Engine II+, all TCAM space on the switch might be exhausted.

  Workaround: None. (CSCed18765)

- When configured for VRF-Lite, a Catalyst 4500 series switch incorrectly forwards packets received on the VRF interface for those destinations not in the VRF routing table. Instead of dropping the packet, the switch forwards the packet using the global routing table.

  Workaround: Enter the **ip route vrf <vrf name> 0.0.0.0 0.0.0.0 null 0** command. (CSCed20990)

- Ports in suspended mode due to misconfiguration in the LACP port channel do not recover, even after reconfiguring the ports. This situation occurs when most ports are configured for dot1q encapsulation and one or more ports are not.

  Workaround: Enter the **switchport trunk encap dot1q** command to add the suspended port to the channel, shut down the port using the **shutdown** command, and then enter the **no shutdown** command to force the port to stay active. This action ensures that the port gets added to the port channel. (CSCeb78999)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays up regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into err-disable mode because of the continuous flapping of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV running Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine running Release 12.1(19)EW (or later). (CSCeb36355)

- If power is denied for an interface, the following console message is printed every five seconds:

  %ILPOWER-5-ILPOWER_POWER_DENY: Interface Gi6/29: inline power denied

  Despite this message, the system is functioning properly.

  Workaround: Turn off logging on the console with the **no logging console** command. (CSCed67157)

- For Release 12.2(18)EW or later, when the Gigabit Ethernet port of a Catalyst 3550 switch with inline power (WS-C3550-25-PWR) is connected to the Gigabit Ethernet port of a Catalyst 4500 series switch with a Supervisor Engine V (WS-X4516), the port on the Catalyst 3500 switch fails POST (power-on self test) during startup.

  Workarounds:

  1. Before starting up the Catalyst 3550 switch, disconnect the cable connecting the uplink ports on the Catalyst 3550 switch to the Catalyst 4500 series switch. Once the Catalyst 3550 switch boots, reconnect the cable.

  2. Before starting up the Catalyst 3550 switch, enter the **shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 series switch. After starting up the Catalyst 3550 switch, enter the **no shutdown** command on the Gigabit Ethernet ports on the Catalyst 4500 switch. (CSCee50578)

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

  Workarounds:

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

  2. Configure the media converter to autonegotiate the speed and duplex instead of running at 100 Mbps and full duplex. (CSCee62109)

Resolved Caveats in Cisco IOS Release 12.2(18)EW1

This section lists the resolved caveats in release 12.2(18)EW1:

- A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

  The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains. (CSCec16481)

Further details and the workarounds to mitigate the effects.

- When Layer 3 fragmentation fails, a Catalyst 4500 series switch running Supervisor Engine IV sends back the wrong ICMP code and causes the Path MTU auto-discovery feature to fail. The switch returns the code “ICMP Host unreachable / Communication administratively filtered (code 13)," yet the correct code is "ICMP Host unreachable / Fragmentation needed but DF-Bit set (Code 4)."

  Workaround: None. (CSCed56513)

- When you upgrade a Cisco IOS software image from Release 12.1(12c) or 12.1(19)E to a release in the 12.2 release train, the following syslog message appears:

  00:00:01: %C4K_IOSSYS-3-BLANKSTARTUPCONFIG: Blank or invalid startup-config, booting up with defaults

  Workaround: The message is harmless and can be ignored. (CSCed26025)

- The **show mod** command will not display the correct status of a WS-X4604-GWY module if the gateway module has failed. The status of the module incorrectly displays as “Ok,” but the correct status is “Offline.” This problem has been resolved in the Release 12.3(8.3)T image of the WS-X4604-GWY module.

  Workaround: Use SNMP to monitor both the gateway module and the supervisor engine as separate devices. (CSCea90578)

Open Caveats in Cisco IOS Release 12.2(18)EW

This section lists the open caveats in Cisco IOS Release 12.2(18)EW.

- When 802.1Q and Layer 2 Protocol Tunneling are disabled on a switch, and the switch is rebooted after saving the configuration, spanning-tree BPDU filtering is not disabled automatically on the port.

  Workaround: Manually disable spanning-tree BPDU filtering on the interface with the **no spanning-tree bpdufilter** command. (CSCec88311)

- When DHCP snooping, IP source guard, and trunks are configured on all 240 interfaces on a Catalyst 4500 series switch equipped with a Supervisor Engine II+, the switch may exhaust its TCAM space.

  Workaround: None. (CSCed18765)

- When Layer 3 fragmentation fails, a Catalyst 4500 series switch running Supervisor Engine IV sends back the wrong ICMP code and causes the Path MTU auto-discovery feature to fail. The switch returns the code “ICMP Host unreachable / Communication administratively filtered (code 13)," yet the correct code is "ICMP Host unreachable / Fragmentation needed but DF-Bit set (Code 4)."

  Workaround: None. (CSCed56513)

- When configured for VRF-Lite, a Catalyst 4500 series switch inadvertently forwards packets received on the VRF interface for those destinations not in the VRF routing table. Instead of dropping the packet, the switch forwards the packet using the global routing table.

  Workaround: Issue the command **ip route vrf <vrf name> 0.0.0.0 0.0.0.0 null 0**. (CSCed20990)

- Ports in suspended mode due to misconfiguration in the LACP port channel do not recover, even after reconfiguring the ports. This situation occurs when most ports are configured for dot1q encapsulation and one or more ports are not.

Workaround: Enter the **switchport trunk encap dot1q** command to add the suspended port to the channel, shut down the port using the **shutdown** command, and then enter the **no shutdown** command to force the port to stay active. This action ensures that the port gets added to the port channel. (CSCeb78999)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays up regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into err-disable mode because of the continuous flapping of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- When you upgrade a Cisco IOS software image from Release 12.1(12c) or 12.1(19)E to a release in the 12.2 release train, the following syslog message appears:
  "00:00:01: %C4K_IOSSYS-3-BLANKSTARTUPCONFIG: Blank or invalid startup-config, booting up with defaults".

  Workaround: Ignore the message. It is harmless. (CSCed26025)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- The **show mod** command will not display the correct status of a WS-X4604-GWY module if the gateway module has crashed. The status of the module incorrectly displays as “Ok,” but the correct status is “Offline.”

  Workaround: Use SNMP to monitor both the gateway module and the supervisor engine as separate devices. (CSCea90578)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV running Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine running Release 12.1(19)EW (or later). (CSCeb36355)

Resolved Caveats in Cisco IOS Release 12.2(18)EW

This section lists the resolved caveats in release 12.2(18)EW:

- The packet memory on a Catalyst 4500 series Supervisor Engine may malfunction. If the packet memory malfunctions, the switch sends data packets with an invalid CRC, and the link partner discards them. Once the problem has been identified by the diagnostics that have been added to detect this problem, the switch automatically shuts down and restarts in "best-effort" mode. In this mode, the affected packet buffers are removed from circulation, and log messages are generated every 30 minutes to alert the user to the failures.

  Workaround: Replace the supervisor engine with packet memory errors. This problem is resolved in Cisco IOS Release 12.2(18)EW. (CSCed61591)

- If you delete an SVI interface that is a member of a VRF (using the **no int vlan 2** command), and then you re-create the interface and assign it to a different VRF, the interface might be treated as if it were still in the original VRF. Subsequently, if you deleted the original VRF, the new VRF configuration might overwrite what is on the SVI.

  Workaround: Erase the VRF configuration from an SVI before deleting it. (CSCec47177)
- Occasionally, when unwanted multicast traffic arrives on an interface on which you did not expect to receive it (also termed an RPF failure), the traffic is dropped. This situation can occur when two multicast routers have active PIM-enabled interfaces on the same Ethernet LAN segment. The PIM protocol ensures that only one router is elected to forward traffic to the LAN segment. The non-forwarding router, however, might still have a multicast route for that same multicast flow. If so, the non-forwarding router creates a multicast "fastdrop" entry in the hardware forwarding table that drops the "RPF failure" packets before they reach the CPU of the non-forwarding router. Normally the **show ip mfib fastdrop** command displays a list of all active fastdrop entries. In some cases the “fastdrop” entry might be displayed.

  Workaround: None. However, you can use the **show ip mfib log** command to validate that the RPF failure packets are not forwarded to the CPU. (CSCec45313)
- If a port is in shutdown state, then the **show interfaces** command might report an incorrect media type. The output of the **show interfaces status** command, however, provides the correct type, even if the port is in shutdown state.

  Workaround: None. (CSCec40451)
- If you have enabled jumbo frames or baby giants, and the switch routes packets destined to a router port (as configured with the **no switchport** command on a WS-X4418-GB or WS-X4412-2GB-T module), the switch might reload when it tries to fragment these packets.

  Workaround: Either disable the jumbo frames or baby giants feature, or remove the WS-X4418-GB or WS-X4412-2GB-T module from the chassis. (CSCec56212)
- When at least 2000 VLAN interfaces are configured in a startup-configuration file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup configuration file. (CSCdx91258)
- If a switchport in loop-inconsistent mode is sending BPDUs and is elected the “designated root” on the segment, the switch will not be able to recover from loop-inconsistent mode.

  Workaround: Disable and then re-enable the switchport. (CSCeb06811)

Open Caveats in Cisco IOS Release 12.1(20)EW4

This section lists the open caveats in Cisco IOS Release 12.1(20)EW4.

- For Cisco IOS Release 12.1(20)EW, in certain scenarios that entail LACP port channels, misconfigured ports do not recover, even after the configuration is fixed. For example, this behavior is observed when you have configured encapsulation on all ports with the **switchport trunk encap dot1q** command. Encapsulation is not configured on the misconfigured port, and the port remains in suspended state, even after the command is re-issued.

  Workaround: Repair the misconfiguration, and then issue a **shutdown** command, followed by a **no shutdown** command. (CSCec57894)
- If you delete an SVI interface that is a member of a VRF (using the **no int vlan 2** command), and then you re-create the interface and assign it to a different VRF, the interface might be treated as if it were still in the original VRF. Subsequently, if you deleted the original VRF, the new VRF configuration might overwrite what is on the SVI.

Workaround: Erase the VRF configuration from an SVI before deleting it. (CSCec47177)

- Occasionally, when unwanted multicast traffic arrives on an interface on which you did not expect to receive it (also termed an RPF failure), the traffic is dropped. This situation can occur when two multicast routers have active PIM-enabled interfaces on the same Ethernet LAN segment. The PIM protocol ensures that only one router is elected to forward traffic to the LAN segment. The non-forwarding router, however, might still have a multicast route for that same multicast flow. If so, the non-forwarding router creates a multicast "fastdrop" entry in the hardware forwarding table that drops the "RPF failure" packets before they reach the CPU of the non-forwarding router. Normally the **show ip mfib fastdrop** command displays a list of all active fastdrop entries. In some cases the "fastdrop" entry might be displayed.

  Workaround: None. However, you can use the **show ip mfib log** command to validate that the RPF failure packets are not forwarded to the CPU. (CSCec45313)

- Occasionally, Enabling auto QoS for the first time might cause the switch to reload.

  Workaround: Issue the **show auto qos interface** command, and then apply all displayed commands manually. (CSCec43783)

- If a port is in shutdown state, then the **show interfaces** command might report an incorrect media type. The output of the **show interfaces status** command, however, provides the correct type, even if the port is in shutdown state.

  Workaround: None. (CSCec40451)

- A spurious error message is appears when the SSH connection disconnects after the IDLE timeout.

  Workaround: Disable IDLE timeouts. (CSCec30214)

- If you have enabled jumbo frames or baby giants, and the switch routes packets destined to a router port (as configured with the **no switchport** command on a WS-X4418-GB or WS-X4412-2GB-T module), the switch might reload when it tries to fragment these packets.

  Workaround: Either disable the jumbo frames or baby giants feature, or remove the WS-X4418-GB or WS-X4412-2GB-T module from the chassis. (CSCec56212)

- When PBR is configured on a Catalyst 4500 Series Switch Supervisor Engine III or IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- When at least 2000 VLAN interfaces are configured in a startup-configuration file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup configuration file. (CSCdx91258)

- The **show mod** command will not reflect the correct status of a WS-X4604-GWY module if the gateway module has crashed. The status of the module is displayed as "Ok," but the status should be "Offline."

  Workaround: Use SNMP to monitor both the gateway module and the supervisor engine as separate devices. (CSCea90578)

- A CompactFlash module formatted on either Supervisor Engine III or IV running Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series supervisor engine running Release 12.1(19)EW (or later). (CSCeb36355)

- If a switchport in loop-inconsistent mode is sending BPDUs and is elected the "designated root" on the segment, the switch will not be able to recover from loop-inconsistent mode.

  Workaround: Disable and then re-enable the switchport. (CSCeb06811)

Resolved Caveats in Cisco IOS Release 12.1(20)EW4

This section lists the resolved caveats in release 12.1(20)EW4:

- Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability. (CSCei76358)
- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  (CSCei61732)

Open Caveats in Cisco IOS Release 12.1(20)EW3

This section lists the open caveats in Cisco IOS Release 12.1(20)EW3.

- For Cisco IOS Release 12.1(20)EW, in certain scenarios that entail LACP port channels, misconfigured ports do not recover, even after the configuration is fixed. For example, this behavior is observed when you have configured encapsulation on all ports with the **switchport trunk encap dot1q** command. Encapsulation is not configured on the misconfigured port, and the port remains in suspended state, even after the command is re-issued.

  Workaround: Repair the misconfiguration, and then issue a **shutdown** command, followed by a **no shutdown** command. (CSCec57894)
- If you delete an SVI interface that is a member of a VRF (using the **no int vlan 2** command), and then you re-create the interface and assign it to a different VRF, the interface might be treated as if it were still in the original VRF. Subsequently, if you deleted the original VRF, the new VRF configuration might overwrite what is on the SVI.

  Workaround: Erase the VRF configuration from an SVI before deleting it. (CSCec47177)
- Occasionally, when unwanted multicast traffic arrives on an interface on which you did not expect to receive it (also termed an RPF failure), the traffic is dropped. This situation can occur when two multicast routers have active PIM-enabled interfaces on the same Ethernet LAN segment. The PIM protocol ensures that only one router is elected to forward traffic to the LAN segment. The non-forwarding router, however, might still have a multicast route for that same multicast flow. If so, the non-forwarding router creates a multicast "fastdrop" entry in the hardware forwarding table that drops the "RPF failure" packets before they reach the CPU of the non-forwarding router. Normally the **show ip mfib fastdrop** command displays a list of all active fastdrop entries. In some cases the “fastdrop” entry might be displayed.

  Workaround: None. However, you can use the **show ip mfib log** command to validate that the RPF failure packets are not forwarded to the CPU. (CSCec45313)
- Occasionally, Enabling auto QoS for the first time might cause the switch to reload.

  Workaround: Issue the **show auto qos interface** command, and then apply all displayed commands manually. (CSCec43783)
- If a port is in shutdown state, then the **show interfaces** command might report an incorrect media type. The output of the **show interfaces status** command, however, provides the correct type, even if the port is in shutdown state.

  Workaround: None. (CSCec40451)

- A spurious error message is appears when the SSH connection disconnects after the IDLE timeout.

  Workaround: Disable IDLE timeouts. (CSCec30214)

- If you have enabled jumbo frames or baby giants, and the switch routes packets destined to a router port (as configured with the **no switchport** command on a WS-X4418-GB or WS-X4412-2GB-T module), the switch might reload when it tries to fragment these packets.

  Workaround: Either disable the jumbo frames or baby giants feature, or remove the WS-X4418-GB or WS-X4412-2GB-T module from the chassis. (CSCec56212)

- When PBR is configured on a Catalyst 4500 Series Switch Supervisor Engine III or IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- When at least 2000 VLAN interfaces are configured in a startup-configuration file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup configuration file. (CSCdx91258)

- The **show mod** command will not reflect the correct status of a WS-X4604-GWY module if the gateway module has crashed. The status of the module is displayed as “Ok,” but the status should be “Offline.”

  Workaround: Use SNMP to monitor both the gateway module and the supervisor engine as separate devices. (CSCea90578)

- A CompactFlash module formatted on either Supervisor Engine III or IV running Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series supervisor engine running Release 12.1(19)EW (or later). (CSCeb36355)

- If a switchport in loop-inconsistent mode is sending BPDUs and is elected the “designated root” on the segment, the switch will not be able to recover from loop-inconsistent mode.

  Workaround: Disable and then re-enable the switchport. (CSCeb06811)

Resolved Caveats in Cisco IOS Release 12.1(20)EW3

This section lists the resolved caveats in release 12.1(20)EW3:

- NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

  ```
  cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
  cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
  cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
  cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
  cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
  cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
  ```

```
cnfFeatureType              1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot              1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive            1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches          1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches          1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges     1.3.6.1.4.1.9.9.99999.1.3.4.1.6
```

(CSCsa81379)

Open Caveats in Cisco IOS Release 12.1(20)EW1

This section lists the open caveats in Cisco IOS Release 12.1(20)EW1.

- For Cisco IOS Release 12.1(20)EW, in certain scenarios that entail LACP port channels, misconfigured ports do not recover, even after the configuration is fixed. For example, this behavior is observed when you have configured encapsulation on all ports with the **switchport trunk encap dot1q** command. Encapsulation is not configured on the misconfigured port, and the port remains in suspended state, even after the command is re-issued.

  Workaround: Repair the misconfiguration, and then issue a **shutdown** command, followed by a **no shutdown** command. (CSCec57894)

- If you delete an SVI interface that is a member of a VRF (using the **no int vlan 2** command), and then you re-create the interface and assign it to a different VRF, the interface might be treated as if it were still in the original VRF. Subsequently, if you deleted the original VRF, the new VRF configuration might overwrite what is on the SVI.

  Workaround: Erase the VRF configuration from an SVI before deleting it. (CSCec47177)

- Occasionally, when unwanted multicast traffic arrives on an interface on which you did not expect to receive it (also termed an RPF failure), the traffic is dropped. This situation can occur when two multicast routers have active PIM-enabled interfaces on the same Ethernet LAN segment. The PIM protocol ensures that only one router is elected to forward traffic to the LAN segment. The non-forwarding router, however, might still have a multicast route for that same multicast flow. If so, the non-forwarding router creates a multicast "fastdrop" entry in the hardware forwarding table that drops the "RPF failure" packets before they reach the CPU of the non-forwarding router. Normally the **show ip mfib fastdrop** command displays a list of all active fastdrop entries. In some cases the “fastdrop” entry might be displayed.

  Workaround: None. However, you can use the **show ip mfib log** command to validate that the RPF failure packets are not forwarded to the CPU. (CSCec45313)

- Occasionally, Enabling auto QoS for the first time might cause the switch to reload.

  Workaround: Issue the **show auto qos interface** command, and then apply all displayed commands manually. (CSCec43783)

- If a port is in shutdown state, then the **show interfaces** command might report an incorrect media type. The output of the **show interfaces status** command, however, provides the correct type, even if the port is in shutdown state.

  Workaround: None. (CSCec40451)

- A spurious error message is appears when the SSH connection disconnects after the IDLE timeout.

  Workaround: Disable IDLE timeouts. (CSCec30214)

- If you have enabled jumbo frames or baby giants, and the switch routes packets destined to a router port (as configured with the **no switchport** command on a WS-X4418-GB or WS-X4412-2GB-T module), the switch might reload when it tries to fragment these packets.

Workaround: Either disable the jumbo frames or baby giants feature, or remove the WS-X4418-GB or WS-X4412-2GB-T module from the chassis. (CSCec56212)

- When PBR is configured on a Catalyst 4500 Series Switch Supervisor Engine III or IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)
- When at least 2000 VLAN interfaces are configured in a startup-configuration file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup configuration file. (CSCdx91258)
- The **show mod** command will not reflect the correct status of a WS-X4604-GWY module if the gateway module has crashed. The status of the module is displayed as “Ok,” but the status should be “Offline.”

  Workaround: Use SNMP to monitor both the gateway module and the supervisor engine as separate devices. (CSCea90578)
- A CompactFlash module formatted on either Supervisor Engine III or IV running Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series supervisor engine running Release 12.1(19)EW (or later). (CSCeb36355)
- If a switchport in loop-inconsistent mode is sending BPDUs and is elected the “designated root” on the segment, the switch will not be able to recover from loop-inconsistent mode.

  Workaround: Disable and then re-enable the switchport. (CSCeb06811)

Resolved Caveats in Cisco IOS Release 12.1(20)EW1

This section lists the resolved caveats in release 12.1(20)EW1:

- Cisco IOS Release 12.1(20)EW1 includes changes that make the Catalyst 4006 and Catalyst 4500 Series chassis 802.3af-ready.

Open Caveats in Cisco IOS Release 12.1(20)EW

This section lists the open caveats in Release 12.1(20)EW.

- For Cisco IOS Release 12.1(20)EW, in certain scenarios that entail LACP port channels, misconfigured ports do not recover, even after the configuration is fixed. For example, this behavior is observed when you have configured encapsulation on all ports with the **switchport trunk encap dot1q** command. Encapsulation is not configured on the misconfigured port, and the port remains in suspended state, even after the command is re-issued.

  Workaround: Repair the misconfiguration, and then issue a **shutdown** command, followed by a **no shutdown** command. (CSCec57894)
- If you delete an SVI interface that is a member of a VRF (using the **no int vlan 2** command), and then re-create the interface and assigned it to a different VRF, it might be treated as if it were still in the original VRF. Subsequently, if you deleted the original VRF, the new VRF configuration might overwrite what is on the SVI.

  Workaround: Erase the VRF configuration from an SVI before deleting it. (CSCec47177)

- Occasionally, when unwanted multicast traffic arrives on an interface on which you did not expect to receive it (also termed an RPF failure), the traffic is dropped. This situation can occur when two multicast routers have active PIM-enabled interfaces on the same Ethernet LAN segment. The PIM protocol ensures that only one router is elected to forward traffic to the LAN segment. The non-forwarding router, however, might still have a multicast route for that same multicast flow. If so, the non-forwarding router creates a multicast "fastdrop" entry in the hardware forwarding table that drops the "RPF failure" packets before they reach the CPU of the non-forwarding router. Normally the **show ip mfib fastdrop** command displays a list of all active fastdrop entries. In some cases the "fastdrop" entry might be displayed.

  Workaround: None. However, you can use the **show ip mfib log** command to validate that the RPF failure packets are not forwarded to the CPU. (CSCec45313)

- Occasionally, when you enable auto QoS for the first time, you might cause the switch to reload.

  Workaround: Issue the command **show auto qos interface**, and then apply all the displayed commands manually. (CSCec43783)

- If a port is in shutdown state, then the **show interfaces** command might report an incorrect media type. The output of the **show interfaces status** command, however, provides the correct type, even if the port is in shutdown state.

  Workaround: None. (CSCec40451)

- A spurious error message is printed when the SSH connection disconnects after the IDLE timeout.

  Workaround: Disable IDLE timeouts. (CSCec30214)

- If you have enabled jumbo frames or baby giants, and the switch routes packets destined to a router port (as configured with **no switchport** on a WS-X4418-GB or WS-X4412-2GB-T module), the switch might reload when it tries to fragment these packets.

  Workaround: Either disable the jumbo frames or baby giants feature, or remove the WS-X4418-GB or WS-X4412-2GB-T module from the chassis. (CSCec56212)

- When PBR is configured on a Catalyst 4500 Supervisor Engine III or IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- When at least 2000 VLAN interfaces are configured in a startup-configuration file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup configuration file. (CSCdx91258)

- The **show mod** command will not reflect the correct status of a WS-X4604-GWY module if the gateway module has crashed. The status of the module is displayed as "Ok"; the status should be "Offline."

  Workaround: Use SNMP to monitor both the gateway module and the supervisor engine as separate devices. (CSCea90578)

- A CompactFlash card formatted on either Supervisor Engine III or IV running Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash card will continue to work on other supervisor engines.

  Workaround: Format the CompactFlash card on any Catalyst 4500 series supervisor engine running 12.1(19)EW (or later).

- If a switchport in loop-inconsistent mode is sending BPDUs and is elected the "designated root" on the segment, it will not be able to recover from loop-inconsistent mode.

  Workaround: Disable and then re-enable the switchport. (CSCeb06811)

Resolved Caveats in Cisco IOS Release 12.1(20)EW

This section lists the resolved caveats in Release 12.1(20)EW:

- When a PortFast-enabled port assumes the forwarding state, it is added to the multicast flood set and starts receiving all unknown multicast traffic. This situation occurs only if the port was previously down and is now up, and IGMP snooping is enabled on that VLAN.

  Workaround: Disable the PortFast feature on the port. (CSCeb33852)

- You cannot update the calendar with the **calendar set** command.

  Workaround: Set the system clock with the **clock set** command, but update the calendar with the **clock update-calendar** command. (CSCea10436)

- Cisco IOS Release 12.1(19)EW can have 10/100 autonegotiation interoperability problems on a WS-X4148-RJ45V (Network Interface Card) that uses the Realtec RTL8139A Chipset.

  Workaround: Turn autonegotiation off. (CSCea18531)

Open Caveats in Cisco IOS Release 12.1(19)EW3

This section lists the open caveats in Release 12.1(19)EW3.

- When PBR is configured on a Catalyst 4500 Supervisor Engine III or IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- When at least 2000 VLAN interfaces are configured in a startup-configuration file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup configuration file. (CSCdx91258)

- The **show mod** command will not reflect the correct status of a WS-X4604-GWY module, if the gateway module has crashed. The status of the module is displayed as “Ok”; the status should be “Offline”.

  Workaround: Use SNMP to monitor both the gateway module and the supervisor engine as separate devices. (CSCea90578)

- When a PortFast-enabled port assumes the forwarding state, it is added to the multicast flood set and starts receiving all unknown multicast traffic. This situation occurs only if the port was previously down and is now up, and IGMP snooping is enabled on that VLAN.

  Workaround: Disable the PortFast feature on the port. (CSCeb33852)

- You cannot update the calendar with the **calendar set** command.

  Workaround: Set the system clock with the **clock set** command, but update the calendar with the **clock update-calendar** command. (CSCea10436)

- A CompactFlash card formatted on either Supervisor Engine III or IV running 12.1E or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash card will continue to work on other supervisor engines.

  Workaround: Format the CompactFlash card on any Catalyst 4500 series supervisor engine running 12.1(19)EW.

- If a switchport in loop-inconsistent mode is sending BPDUs and is elected the “designated root” on the segment, it will not be able to recover from loop-inconsistent mode.

  Workaround: Disable and then reenable the switchport. (CSCeb06811)

- Release 12.1(19)EW can have 10/100 autonegotiation interoperability problems on a WS-X4148-RJ45V (Network Interface Card) that uses the Realtec RTL8139A Chipset.

  Workaround: Turn autonegotiation off. (CSCea18531)
- The **interface range** command is incompatible with the **no ip igmp snooping tcn flood** command.

  Workaround: Apply the CLI directly on the interface. (CSCeb33811)

Resolved Caveats in Cisco IOS Release 12.1(19)EW3

This section lists the resolved caveats in Release 12.1(19)EW3:

- Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability. (CSCei76358)
- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  (CSCei61732)

Open Caveats in Cisco IOS Release 12.1(19)EW2

This section lists the open caveats in Release 12.1(19)EW2.

- When PBR is configured on a Catalyst 4500 Supervisor Engine III or IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)
- When at least 2000 VLAN interfaces are configured in a startup-configuration file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup configuration file. (CSCdx91258)
- The **show mod** command will not reflect the correct status of a WS-X4604-GWY module, if the gateway module has crashed. The status of the module is displayed as “Ok”; the status should be “Offline”.

  Workaround: Use SNMP to monitor both the gateway module and the supervisor engine as separate devices. (CSCea90578)
- When a PortFast-enabled port assumes the forwarding state, it is added to the multicast flood set and starts receiving all unknown multicast traffic. This situation occurs only if the port was previously down and is now up, and IGMP snooping is enabled on that VLAN.

  Workaround: Disable the PortFast feature on the port. (CSCeb33852)
- You cannot update the calendar with the **calendar set** command.

  Workaround: Set the system clock with the **clock set** command, but update the calendar with the **clock update-calendar** command. (CSCea10436)
- A CompactFlash card formatted on either Supervisor Engine III or IV running 12.1E or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash card will continue to work on other supervisor engines.

Workaround: Format the CompactFlash card on any Catalyst 4500 series supervisor engine running 12.1(19)EW.

- If a switchport in loop-inconsistent mode is sending BPDUs and is elected the "designated root" on the segment, it will not be able to recover from loop-inconsistent mode.

  Workaround: Disable and then reenable the switchport. (CSCeb06811)

- Release 12.1(19)EW can have 10/100 autonegotiation interoperability problems on a WS-X4148-RJ45V (Network Interface Card) that uses the Realtec RTL8139A Chipset.

  Workaround: Turn autonegotiation off. (CSCea18531)

- The **interface range** command is incompatible with the **no ip igmp snooping tcn flood** command.

  Workaround: Apply the CLI directly on the interface. (CSCeb33811)

Resolved Caveats in Cisco IOS Release 12.1(19)EW2

This section lists the resolved caveats in Release 12.1(19)EW2:

- NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

```
cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType                1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot                1.3.6.1.4.1.9.9.99999.1.3.4.1.2
```

Open Caveats in Cisco IOS Release 12.1(19)EW1

This section lists the open caveats in Release 12.1(19)EW1.

- When PBR is configured on a Catalyst 4500 Supervisor Engine III or IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- When at least 2000 VLAN interfaces are configured in a startup-configuration file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup configuration file. (CSCdx91258)

- The **show mod** command will not reflect the correct status of a WS-X4604-GWY module, if the gateway module has crashed. The status of the module is displayed as “Ok”; the status should be “Offline”.

  Workaround: Use SNMP to monitor both the gateway module and the supervisor engine as separate devices. (CSCea90578)
- When a PortFast-enabled port assumes the forwarding state, it is added to the multicast flood set and starts receiving all unknown multicast traffic. This situation occurs only if the port was previously down and is now up, and IGMP snooping is enabled on that VLAN.

  Workaround: Disable the PortFast feature on the port. (CSCeb33852)
- You cannot update the calendar with the **calendar set** command.

  Workaround: Set the system clock with the **clock set** command, but update the calendar with the **clock update-calendar** command. (CSCea10436)
- A CompactFlash card formatted on either Supervisor Engine III or IV running 12.1E or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash card will continue to work on other supervisor engines.

  Workaround: Format the CompactFlash card on any Catalyst 4500 series supervisor engine running 12.1(19)EW.
- If a switchport in loop-inconsistent mode is sending BPDUs and is elected the “designated root” on the segment, it will not be able to recover from loop-inconsistent mode.

  Workaround: Disable and then reenable the switchport. (CSCeb06811)
- Release 12.1(19)EW can have 10/100 autonegotiation interoperability problems on a WS-X4148-RJ45V (Network Interface Card) that uses the Realtec RTL8139A Chipset.

  Workaround: Turn autonegotiation off. (CSCea18531)
- The **interface range** command is incompatible with the **no ip igmp snooping tcn flood** command.

  Workaround: Apply the CLI directly on the interface. (CSCeb33811)

Resolved Caveats in Cisco IOS Release 12.1(19)EW1

This section lists the resolved caveats in Release 12.1(19)EW1:

- When the ports on a WS-X4448-GB-LX module are connected and the link is up, the online diagnostics loopback test fails during bootup and the failed ports are marked as faulty.

  If all the ports on a stub are connected during bootup, the loopback test indicates a stub failure and the ports will neither come up nor switch traffic.

  Workaround: Do one of the following:

  - Unplug the fiber or SFPs from the ports on the module before bootup and reconnect them after the module is online.
  - Disable the link partner for all connected ports on the module before bootup and reenable the link partner after the module is online. (CSCeb59072)
- The **show interface flowcontrol** command will crash the switch if a portchannel has been created and then deleted previously.

  Workaround: None. (CSCeb61931)

- IGMPv3 leaves are not being forwarded to the multicast router ports, which impacts bandwidth by delaying the pruning of traffic from the router to the host. The result is unwanted multicast traffic between the router and the switch, which remains longer than necessary. The problem is corrected when the router "ages out" the interface from the group, which usually occurs on the router's next IGMP general query.

  When multiple group records are present in an IGMPv3 membership report and the last record is a leave, the entire membership report will not be sent to the multicast router ports. This behavior might cause you to lose a v3 join.

  Workaround: None. (CSCeb60069)

- If one of two collocated hosts has sent an IGMP leave for the group, the ports on the other host might experience multicast disconnection for up to 5 seconds.

  Workaround: None. (CSCeb45371)

- When you enable DHCP snooping and configure a static MAC drop entry for a router or DHCP client, the switch might shut down.

  Workaround: When DHCP snooping is enabled, do not configure a static MAC drop entry, such as the following:

  ```
  mac-address-table static 00aa.00bb.00cc vlan 100 drop
  ```
  aa.bb.cc is a MAC address for either a router or a DHCP client. (CSCeb62361)

- If you have previously configured an access port with static MAC address (for example, through port security) and now you attempt to enable an IP Source Guard MAC filter, the switch may reload.

  Workaround: Either enable IP Source Guard with IP filter only, or ensure that there is no static MAC address entry configured on the port. (CSCeb74573)

- With a URT-based dynamic VLAN assignment for VMPs, a supervisor engine running 12.1(19)EW may reset.

  Workaround: None. (CSCeb62034)

Open Caveats in Cisco IOS Release 12.1(19)EW

This section lists the open caveats in Release 12.1(19)EW.

- When the ports on a WS-X4448-GB-LX module are connected and the link is up, the online diagnostics loopback test fails during bootup and the failed ports are marked as faulty.

  If all the ports on a stub are connected during bootup, the loopback test indicates a stub failure and the ports will neither come up nor switch traffic.

  Workaround: Do one of the following:

  - Unplug the fiber or SFPs from the ports on the module before bootup and reconnect them after the module is online.
  - Disable the link partner for all connected ports on the module before bootup and reenable the link partner after the module is online. (CSCeb59072)

- The **show interface flowcontrol** command will crash the switch if a portchannel has been created and then deleted previously.

  Workaround: None. (CSCeb61931)

- IGMPv3 leaves are not being forwarded to the multicast router ports, which impacts bandwidth by delaying the pruning of traffic from the router to the host. The result is unwanted multicast traffic between the router and the switch, which remains longer than necessary. The problem is corrected when the router “ages out” the interface from the group, which usually occurs on the router’s next IGMP general query.

  When multiple group records are present in an IGMPv3 membership report and the last record is a leave, the entire membership report will not be sent to the multicast router ports. This behavior might cause you to lose a v3 join.

  Workaround: None. (CSCeb60069)

- If one of two collocated hosts has sent an IGMP leave for the group, the ports on the other host might experience multicast disconnection for up to 5 seconds.

  Workaround: None. (CSCeb45371)

- When you enable DHCP snooping and configure a static MAC drop entry for a router or DHCP client, the switch might shut down.

  Workaround: When DHCP snooping is enabled, do not configure a static MAC drop entry, such as the following:

  ```
  mac-address-table static 00aa.00bb.00cc vlan 100 drop
  ```

  aa.bb.cc is a MAC address for either a router or a DHCP client. (CSCeb62361)

- If you have previously configured an access port with static MAC address (for example, through port security) and now you attempt to enable an IP Source Guard MAC filter, the switch may reload.

  Workaround: Either enable IP Source Guard with IP filter only, or ensure that there is no static MAC address entry configured on the port. (CSCeb74573)

- With a URT-based dynamic VLAN assignment for VMPs, a supervisor engine running 12.1(19)EW may reset.

  Workaround: None. (CSCeb62034)

- When PBR is configured on a Catalyst 4500 Supervisor Engine III or IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- When at least 2000 VLAN interfaces are configured in a startup-configuration file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup configuration file. (CSCdx91258)

- The **show mod** command will not reflect the correct status of a WS-X4604-GWY module, if the gateway module has crashed. The status of the module is displayed as “Ok”; the status should be “Offline.”

  Workaround: Use SNMP to monitor both the gateway module and the supervisor engine as separate devices. (CSCea90578)

- When a PortFast-enabled port assumes the forwarding state, it is added to the multicast flood set and starts receiving all unknown multicast traffic. This situation occurs only if the port was previously down and is now up, and IGMP snooping is enabled on that VLAN.

  Workaround: Disable the PortFast feature on the port. (CSCeb33852)

- You cannot update the calendar with the **calendar set** command.

  Workaround: Set the system clock with the **clock set** command, but update the calendar with the **clock update-calendar** command. (CSCea10436)

- A CompactFlash card formatted on either Supervisor Engine III or IV running 12.1E or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash card will continue to work on other supervisor engines.

  Workaround: Format the CompactFlash card on any Catalyst 4500 series supervisor engine running 12.1(19)EW.
- If a switchport in loop-inconsistent mode is sending BPDUs and is elected the "designated root" on the segment, it will not be able to recover from loop-inconsistent mode.

  Workaround: Disable and then reenable the switchport. (CSCeb06811)
- Release 12.1(19)EW can have 10/100 autonegotiation interoperability problems on a WS-X4148-RJ45V (Network Interface Card) that uses the Realtec RTL8139A Chipset.

  Workaround: Turn autonegotiation off. (CSCea18531)
- The **interface range** command is incompatible with the **no ip igmp snooping tcn flood** command.

  Workaround: Apply the CLI directly on the interface. (CSCeb33811)

Resolved Caveats in Cisco IOS Release 12.1(19)EW

This section lists the resolved caveats in Release 12.1(19)EW:

- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. (CSCdu53656 and CSCea28131)
- Catalyst 4500 IOS supervisor engines exhibit slow IPX routing performance (high latency).

  Workaround: None. (CSCea85204)
- When oversubscribed traffic destined for queue 4 is dropped in queue 4, the dynamic buffer limiting (DBL) drop counters for queue 2 (seen when you enter the **show int <int> counter** command) are incremented. When oversubscribed traffic destined for queue 2 is dropped in queue 2, the DBL drop counters for queue 4 are incremented.

  Queues 1 and 3 perform correctly.

  Workaround: None. (CSCdz58560)
- When IGMP Snooping is enabled and the last member leaves a multicast group, the switch will send an IGMP leave message with the source IP address of 0.0.0.0.

  Workaround: None. (CSCdz49171)
- When a fan tray fails or is removed, the supervisor engine status may not register as faulty and the status LED may not turn amber. The status LED also may not turn red when the power supply fails or is removed.

  Workaround: None. (CSCdz55274)
- When a nonblocking gigaport is configured as "unidirectional receive-only" and as "speed nonegotiation," the port link may not come up after both CLIs are unconfigured.

  Workaround: Do one of the following:

  - Avoid configuring both unidirectional receive-only and speed nonegotiation on the same port, because the former places a port in speed nonegotiation mode.

  - Enter the **shut** and **no shut** commands to reset the port's link partner and bring up the port's link. (CSCdz53781)

- When the fan tray is removed from the switch for more than 5 minutes, the following message is displayed on the console and all line cards are reset:

  ```
  %C4K_CHASSIS-2-INSUFFICIENTFANSDETECTED: Too few working fans, the chassis will
  overheat
  ```
  Workaround: None. (CSCdz50817)

- When a Catalyst 4500 Supervisor Engine III or IV is configured to use PBR, and the route map specifies that the action is a default next-hop, that action is taken only if the ARP resolution for the specified host has already taken place. If the ARP resolution has not taken place, the system does not consider the host to be a valid default next-hop.

  Workaround: Ping the specified host to ensure that it is always in the ARP table. (CSCdz50786)

- If none of a port channel's ports support jumbo frames, your attempt to change the MTU on the port channel will change the port channels MTU, but not the member ports MTU. None of the member ports are suspended.

  If some of the member ports support jumbo frames, this situation does not happen and the ports that do not support jumbo frames are suspended.

  Workaround: Do not change the port channel's MTU if none of its member ports support jumbo frames. (CSCdz43350)

- When the WS-X4148-RJ45V card is plugged into a Catalyst 4500 chassis, the power on LED does not operate. This caveat is present in 12.1(13)EW and all previous software releases.

  Workaround: None. (CSCdz60995)

- Disabling IGMP snooping with a large number of groups and VLANs might cause CPU HOG and HOST FLAPPING. If so, you will see messages similar to the following on the console:

  ```
  %SYS-3-CPUHOG: Task ran for 8692 msec (0/0), process = Exec, PC = 128790.
  %C4K_EBM-4-HOSTFLAPPING: Host 00:10:0B:10:B9:20 in vlan 200 is flapping between port
  Po2 and port Po1
  ```
  Workaround: None. (CSCdy21031)

- When the spanning tree mode is PVST, isolated trunk ports transmit BPDUs with the primary VLAN instead of the secondary VLAN.

  Workaround: Use the **spanning-tree bpduguard enable** interface command to enable BPDU Guard to detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the **shutdown** VLAN configuration command and reenabled using the **no shutdown** VLAN configuration command, any subsequent flooded or multicast packets received on the private VLAN port does not reach all the destinations.

  Workaround: Do not use the **shutdown** and **no shutdown** VLAN configuration command to disable the VLAN. Delete and recreate the secondary VLAN with the proper VLAN type and association configuration. (CSCdy22082)

- When a VLAN filter is applied to filter IP traffic based on Layer 4 information, fragmented packets might not be filtered correctly. Only the initial fragment has all the Layer 4 information. Noninitial fragments do not have any Layer 4 information (for example, UDP ports and the TCP flag).

  Workaround: If IP packets can be fragmented in your network, program ACLs in the VLAN map, without any Layer 4 information. (CSCdx84696)

- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Open Caveats in Cisco IOS Release 12.1(13)EW4

This section lists the open caveats in Release 12.1(13)EW4.

- When oversubscribed traffic destined for queue 4 is dropped in queue 4, the DBL drop counters for queue 2 (seen when the **show int <int> counter** command is issued) are incremented. When oversubscribed traffic destined for queue 2 is dropped in queue 2, the DBL drop counters for queue 4 are incremented.

  Queues 1 and 3 perform correctly.

  Workaround: None. (CSCdz58560)
- When IGMP Snooping is enabled and the last member leaves a multicast group, the switch will send an IGMP leave message with the source IP address of 0.0.0.0.

  Workaround: None. (CSCdz49171)
- Supervisor engine status may not register as faulty and the status LED may not turn amber when a fan-tray fails or is removed. Moreover, the status LED may not go turn red when the power supply fails or is removed.

  Workaround: None. (CSCdz55274)
- When a non-blocking gigaport is configured as “unidirectional receive-only” as well as “speed nonegotiation,” once both CLIs are unconfigured, the port link may not come up.

  Workaround: Do one of the following:

  - Avoid configuring both unidirectional receive-only and speed nonegotiation on the same port, because the former places a port in speed nonegotiation mode.
  - Issue **shut** and **no shut** commands to reset the port’s link partner and bring up the port's link. (CSCdz53781)
- When the fan tray is removed from the switch for more than 5 minutes, the following message is displayed on the console and all line cards are reset:

  ```
  %C4K_CHASSIS-2-INSUFFICIENTFANSDETECTED: Too few working fans, the chassis will
  overheat
  ```

  Workaround: None. (CSCdz50817)
- When a Catalyst 4000 Supervisor Engine III or IV is configured to use PBR, and the route-map specifies that the action is a default next-hop, that action is taken only if the ARP resolution for the specified host has already taken place. If the ARP resolution has not taken place, the system does not consider the host to be a valid default next-hop.

  Workaround: Ping the specified host to ensure that it is always in the ARP table. (CSCdz50786)
- If none of a port-channel’s ports support Jumbo Frame, your attempt to change the MTU on the port-channel will change the port-channel's MTU, but not the member ports' MTU. Moreover, none of the member ports are suspended.

  In contrast, if some of the member ports support jumbo frames, this scenario does not happen and the ports that do not support jumbo frames are suspended.

Workaround: Do not change the port-channel's MTU if none of its member ports support jumbo frames. (CSCdz43350)

- When PBR is configured on a Catalyst 4000 Supervisor Engine III or IV, PBR packets switched by hardware update the access-list or route-map statistics improperly.

  Workaround: None. (CSCdz10171)

- When the WS-X4148-RJ45V card is plugged into a Catalyst 4500 chassis, the power LED “on” does not work. This caveat is present in 12.1(13)EW and all previous software releases.

  Workaround: None. (CSCdz60995)

- With at least 2000 VLAN interfaces configured in the startup-config file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup config file. (CSCdx91258)

- Disabling IGMP snooping with a large number of groups and VLANs might cause CPU HOG and HOST FLAPPING. If so, you will see messages like the following on the console:

  ```
  %SYS-3-CPUHOG: Task ran for 8692 msec (0/0), process = Exec, PC = 128790.
  %C4K_EBM-4-HOSTFLAPPING: Host 00:10:0B:10:B9:20 in vlan 200 is flapping between port
  Po2 and port Po1
  ```

  Workaround: None. (CSCdy21031)

- When the spanning tree mode is PVST, isolated trunk ports transmit BPDUs with the primary VLAN instead of the secondary VLAN.

  Workaround: Use the **spanning-tree bpduguard enable** interface command to enable BPDU Guard to detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the **shutdown** VLAN configuration command and re-enabled using the **no shutdown** VLAN configuration command, any subsequent flooded/multicast packets received on the private VLAN port does not reach all the destinations.

  Workaround: Do not use the **shutdown** and **no shutdown** VLAN configuration command to disable the VLAN. Instead, delete and recreate the secondary VLAN with the proper VLAN type and association configuration. (CSCdy22082)

- When a VLAN filter is applied to filter IP traffic based on Layer 4 information, fragmented packets might not be filtered correctly. Only the initial fragment has all the Layer 4 information. Non-initial fragments do not have any Layer 4 information (e.g., UDP ports, TCP flag, etc.).

  Workaround: If IP packets can be fragmented in your network, program ACLs in the VLAN Map, without any Layer 4 information. (CSCdx84696)

- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Resolved Caveats in Cisco IOS Release 12.1(13)EW4

This section lists the resolved caveats in Release 12.1(13)EW4.

- Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability. (CSCei76358)

- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  (CSCei61732)

Open Caveats in Cisco IOS Release 12.1(13)EW3

This section lists the open caveats in Release 12.1(13)EW3.

- When oversubscribed traffic destined for queue 4 is dropped in queue 4, the DBL drop counters for queue 2 (seen when the **show int <int> counter** command is issued) are incremented. When oversubscribed traffic destined for queue 2 is dropped in queue 2, the DBL drop counters for queue 4 are incremented.

  Queues 1 and 3 perform correctly.

  Workaround: None. (CSCdz58560)

- When IGMP Snooping is enabled and the last member leaves a multicast group, the switch will send an IGMP leave message with the source IP address of 0.0.0.0.

  Workaround: None. (CSCdz49171)

- Supervisor engine status may not register as faulty and the status LED may not turn amber when a fan-tray fails or is removed. Moreover, the status LED may not go turn red when the power supply fails or is removed.

  Workaround: None. (CSCdz55274)

- When a non-blocking gigaport is configured as “unidirectional receive-only” as well as “speed nonegotiation,” once both CLIs are unconfigured, the port link may not come up.

  Workaround: Do one of the following:

  - Avoid configuring both unidirectional receive-only and speed nonegotiation on the same port, because the former places a port in speed nonegotiation mode.
  - Issue **shut** and **no shut** commands to reset the port’s link partner and bring up the port's link. (CSCdz53781)

- When the fan tray is removed from the switch for more than 5 minutes, the following message is displayed on the console and all line cards are reset:

  ```
  %C4K_CHASSIS-2-INSUFFICIENTFANSDETECTED: Too few working fans, the chassis will
  overheat
  ```

  Workaround: None. (CSCdz50817)

- When a Catalyst 4000 Supervisor Engine III or IV is configured to use PBR, and the route-map specifies that the action is a default next-hop, that action is taken only if the ARP resolution for the specified host has already taken place. If the ARP resolution has not taken place, the system does not consider the host to be a valid default next-hop.

  Workaround: Ping the specified host to ensure that it is always in the ARP table. (CSCdz50786)

- If none of a port-channel’s ports support Jumbo Frame, your attempt to change the MTU on the port-channel will change the port-channel's MTU, but not the member ports' MTU. Moreover, none of the member ports are suspended.

In contrast, if some of the member ports support jumbo frames, this scenario does not happen and the ports that do not support jumbo frames are suspended.

Workaround: Do not change the port-channel's MTU if none of its member ports support jumbo frames. (CSCdz43350)

- When PBR is configured on a Catalyst 4000 Supervisor Engine III or IV, PBR packets switched by hardware update the access-list or route-map statistics improperly.

  Workaround: None. (CSCdz10171)

- When the WS-X4148-RJ45V card is plugged into a Catalyst 4500 chassis, the power LED “on” does not work. This caveat is present in 12.1(13)EW and all previous software releases.

  Workaround: None. (CSCdz60995)

- With at least 2000 VLAN interfaces configured in the startup-config file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup config file. (CSCdx91258)

- Disabling IGMP snooping with a large number of groups and VLANs might cause CPU HOG and HOST FLAPPING. If so, you will see messages like the following on the console:

  ```
  %SYS-3-CPUHOG: Task ran for 8692 msec (0/0), process = Exec, PC = 128790.
  %C4K_EBM-4-HOSTFLAPPING: Host 00:10:0B:10:B9:20 in vlan 200 is flapping between port
  Po2 and port Po1
  ```

  Workaround: None. (CSCdy21031)

- When the spanning tree mode is PVST, isolated trunk ports transmit BPDUs with the primary VLAN instead of the secondary VLAN.

  Workaround: Use the **spanning-tree bpduguard enable** interface command to enable BPDU Guard to detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the **shutdown** VLAN configuration command and re-enabled using the **no shutdown** VLAN configuration command, any subsequent flooded/multicast packets received on the private VLAN port does not reach all the destinations.

  Workaround: Do not use the **shutdown** and **no shutdown** VLAN configuration command to disable the VLAN. Instead, delete and recreate the secondary VLAN with the proper VLAN type and association configuration. (CSCdy22082)

- When a VLAN filter is applied to filter IP traffic based on Layer 4 information, fragmented packets might not be filtered correctly. Only the initial fragment has all the Layer 4 information. Non-initial fragments do not have any Layer 4 information (e.g., UDP ports, TCP flag, etc.).

  Workaround: If IP packets can be fragmented in your network, program ACLs in the VLAN Map, without any Layer 4 information. (CSCdx84696)

- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Resolved Caveats in Cisco IOS Release 12.1(13)EW3

This section lists the resolved caveats in Release 12.1(13)EW3.

- NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

  ```
  cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
  cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
  cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
  cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
  cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
  cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
  cnfFeatureType                1.3.6.1.4.1.9.9.99999.1.3.4.1.1
  cnfFeatureSlot                1.3.6.1.4.1.9.9.99999.1.3.4.1.2
  cnfFeatureActive              1.3.6.1.4.1.9.9.99999.1.3.4.1.3
  cnfFeatureAttaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.4
  cnfFeatureDetaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.5
  cnfFeatureConfigChanges       1.3.6.1.4.1.9.9.99999.1.3.4.1.6
  ```

  (CSCsa81379)

Open Caveats in Cisco IOS Release 12.1(13)EW2

This section lists the open caveats in Release 12.1(13)EW2.

- When oversubscribed traffic destined for queue 4 is dropped in queue 4, the DBL drop counters for queue 2 (seen when the **show int <int> counter** command is issued) are incremented. When oversubscribed traffic destined for queue 2 is dropped in queue 2, the DBL drop counters for queue 4 are incremented.

  Queues 1 and 3 perform correctly.

  Workaround: None. (CSCdz58560)

- When IGMP Snooping is enabled and the last member leaves a multicast group, the switch will send an IGMP leave message with the source IP address of 0.0.0.0.

  Workaround: None. (CSCdz49171)

- Supervisor engine status may not register as faulty and the status LED may not turn amber when a fan-tray fails or is removed. Moreover, the status LED may not go turn red when the power supply fails or is removed.

  Workaround: None. (CSCdz55274)

- When a non-blocking gigaport is configured as “unidirectional receive-only” as well as “speed nonegotiation,” once both CLIs are unconfigured, the port link may not come up.

Workaround: Do one of the following:

- Avoid configuring both unidirectional receive-only and speed nonegotiation on the same port, because the former places a port in speed nonegotiation mode.
- Issue **shut** and **no shut** commands to reset the port's link partner and bring up the port's link. (CSCdz53781)

- When the fan tray is removed from the switch for more than 5 minutes, the following message is displayed on the console and all line cards are reset:

```
%C4K_CHASSIS-2-INSUFFICIENTFANSDETECTED: Too few working fans, the chassis will
overheat
```

  Workaround: None. (CSCdz50817)

- When a Catalyst 4000 Supervisor Engine III or IV is configured to use PBR, and the route-map specifies that the action is a default next-hop, that action is taken only if the ARP resolution for the specified host has already taken place. If the ARP resolution has not taken place, the system does not consider the host to be a valid default next-hop.

  Workaround: Ping the specified host to ensure that it is always in the ARP table. (CSCdz50786)

- If none of a port-channel's ports support Jumbo Frame, your attempt to change the MTU on the port-channel will change the port-channel's MTU, but not the member ports' MTU. Moreover, none of the member ports are suspended.

  In contrast, if some of the member ports support jumbo frames, this scenario does not happen and the ports that do not support jumbo frames are suspended.

  Workaround: Do not change the port-channel's MTU if none of its member ports support jumbo frames. (CSCdz43350)

- When PBR is configured on a Catalyst 4000 Supervisor Engine III or IV, PBR packets switched by hardware update the access-list or route-map statistics improperly.

  Workaround: None. (CSCdz10171)

- When the WS-X4148-RJ45V card is plugged into a Catalyst 4500 chassis, the power LED "on" does not work. This caveat is present in 12.1(13)EW and all previous software releases.

  Workaround: None. (CSCdz60995)

- With at least 2000 VLAN interfaces configured in the startup-config file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup config file. (CSCdx91258)

- Disabling IGMP snooping with a large number of groups and VLANs might cause CPU HOG and HOST FLAPPING. If so, you will see messages like the following on the console:

```
%SYS-3-CPUHOG: Task ran for 8692 msec (0/0), process = Exec, PC = 128790.
%C4K_EBM-4-HOSTFLAPPING: Host 00:10:0B:10:B9:20 in vlan 200 is flapping between port
Po2 and port Po1
```

  Workaround: None. (CSCdy21031)

- When the spanning tree mode is PVST, isolated trunk ports transmit BPDUs with the primary VLAN instead of the secondary VLAN.

  Workaround: Use the **spanning-tree bpduguard enable** interface command to enable BPDU Guard to detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the **shutdown** VLAN configuration command and re-enabled using the **no shutdown** VLAN configuration command, any subsequent flooded/multicast packets received on the private VLAN port does not reach all the destinations.

Workaround: Do not use the **shutdown** and **no shutdown** VLAN configuration command to disable the VLAN. Instead, delete and recreate the secondary VLAN with the proper VLAN type and association configuration. (CSCdy22082)

- When a VLAN filter is applied to filter IP traffic based on Layer 4 information, fragmented packets might not be filtered correctly. Only the initial fragment has all the Layer 4 information. Non-initial fragments do not have any Layer 4 information (e.g., UDP ports, TCP flag, etc.).

  Workaround: If IP packets can be fragmented in your network, program ACLs in the VLAN Map, without any Layer 4 information. (CSCdx84696)

- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Resolved Caveats in Cisco IOS Release 12.1(13)EW2

This section lists the resolved caveats in Release 12.1(13)EW2.

- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Workaround: Cisco has made software available, free of charge, to correct the problem. (CSCdz71127)

  This advisory is available at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030717-blocked

- Under certain conditions, a caveat in the power on self test (POST) may erroneously indicate that good WS-X4014 and WS-X4515 supervisor engines are faulty. When this happens, modules do not come online and the switch cannot be used to forward traffic.

  If the POST incorrectly identifies a good supervisor engine as faulty because of this situation, the POST output will only display the first port on the switch as faulty:

  ```
  Port Traffic: L2 Serdes Loopback ...
  0: F  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
  12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
  24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: .
  ```

  If the POST fails, but the test output does not match the display shown here, your hardware probably is faulty.

  This POST behavior is a software issue and has been resolved in 12.1(12c)EW2, 12.1(13)EW2, 12.1(19)EW, and 12.1(20)E images.

  Workaround: None. (CSCeb59442)

Open Caveats in Cisco IOS Release 12.1(13)EW1

This section lists the open caveats in Release 12.1(13)EW1.

- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Workaround: Cisco has made software available, free of charge, to correct the problem. (CSCdz71127)

  This advisory is available at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030717-blocked

- Under certain conditions, a caveat in the power on self test (POST) may erroneously indicate that good WS-X4014 and WS-X4515 supervisor engines are faulty. When this happens, modules do not come online and the switch cannot be used to forward traffic.

  If the POST incorrectly identifies a good supervisor engine as faulty because of this situation, the POST output will only display the first port on the switch as faulty:

  ```
  Port Traffic: L2 Serdes Loopback ...
  0: F  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
  12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
  24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: .
  ```

  If the POST fails, but the test output does not match the display shown here, your hardware probably is faulty.

  This POST behavior is a software issue and has been resolved in 12.1(12c)EW2, 12.1(13)EW2, 12.1(19)EW, and 12.1(20)E images.

  Workaround: None. (CSCeb59442)

- When oversubscribed traffic destined for queue 4 is dropped in queue 4, the DBL drop counters for queue 2 (seen when the **show int <int> counter** command is issued) are incremented. When oversubscribed traffic destined for queue 2 is dropped in queue 2, the DBL drop counters for queue 4 are incremented.

  Queues 1 and 3 perform correctly.

  Workaround: None. (CSCdz58560)

- When IGMP Snooping is enabled and the last member leaves a multicast group, the switch will send an IGMP leave message with the source IP address of 0.0.0.0.

  Workaround: None. (CSCdz49171)

- Supervisor engine status may not register as faulty and the status LED may not turn amber when a fan-tray fails or is removed. Moreover, the status LED may not go turn red when the power supply fails or is removed.

  Workaround: None. (CSCdz55274)

- When a non-blocking gigaport is configured as “unidirectional receive-only” as well as “speed nonegotiation,” once both CLIs are unconfigured, the port link may not come up.

Workaround: Do one of the following:

- Avoid configuring both unidirectional receive-only and speed nonegotiation on the same port, because the former places a port in speed nonegotiation mode.
- Issue **shut** and **no shut** commands to reset the port’s link partner and bring up the port's link. (CSCdz53781)

- When the fan tray is removed from the switch for more than 5 minutes, the following message is displayed on the console and all line cards are reset:

```
%C4K_CHASSIS-2-INSUFFICIENTFANSDETECTED: Too few working fans, the chassis will
overheat
```

  Workaround: None. (CSCdz50817)

- When a Catalyst 4000 Supervisor Engine III or IV is configured to use PBR, and the route-map specifies that the action is a default next-hop, that action is taken only if the ARP resolution for the specified host has already taken place. If the ARP resolution has not taken place, the system does not consider the host to be a valid default next-hop.

  Workaround: Ping the specified host to ensure that it is always in the ARP table. (CSCdz50786)

- If none of a port-channel’s ports support Jumbo Frame, your attempt to change the MTU on the port-channel will change the port-channel's MTU, but not the member ports' MTU. Moreover, none of the member ports are suspended.

  In contrast, if some of the member ports support jumbo frames, this scenario does not happen and the ports that don't support jumbo frames are suspended.

  Workaround: Do not change the port-channel's MTU if none of its member ports support jumbo frames. (CSCdz43350)

- When PBR is configured on a Catalyst 4000 Supervisor Engine III or IV, PBR packets switched by hardware update the access-list or route-map statistics improperly.

  Workaround: None. (CSCdz10171)

- When the WS-X4148-RJ45V card is plugged into a Catalyst 4500 chassis, the power LED “on” does not work. This caveat is present in 12.1(13)EW and all previous software releases.

  Workaround: None. (CSCdz60995)

- With at least 2000 VLAN interfaces configured in the startup-config file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup config file. (CSCdx91258)

- Disabling IGMP snooping with a large number of groups and VLANs might cause CPU HOG and HOST FLAPPING. If so, you will see messages like the following on the console:

```
%SYS-3-CPUHOG: Task ran for 8692 msec (0/0), process = Exec, PC = 128790.
%C4K_EBM-4-HOSTFLAPPING: Host 00:10:0B:10:B9:20 in vlan 200 is flapping between port
Po2 and port Po1
```

  Workaround: None. (CSCdy21031)

- When the spanning tree mode is PVST, isolated trunk ports transmit BPDUs with the primary VLAN instead of the secondary VLAN.

  Workaround: Use the **spanning-tree bpduguard enable** interface command to enable BPDU Guard to detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the **shutdown** VLAN configuration command and re-enabled using the **no shutdown** VLAN configuration command, any subsequent flooded/multicast packets received on the private VLAN port does not reach all the destinations.

Workaround: Do not use the **shutdown** and **no shutdown** VLAN configuration command to disable the VLAN. Instead, delete and recreate the secondary VLAN with the proper VLAN type and association configuration. (CSCdy22082)

- When a VLAN filter is applied to filter IP traffic based on Layer 4 information, fragmented packets might not be filtered correctly. Only the initial fragment has all the Layer 4 information. Non-initial fragments do not have any Layer 4 information (e.g., UDP ports, TCP flag, etc.).

  Workaround: If IP packets can be fragmented in your network, program ACLs in the VLAN Map, without any Layer 4 information. (CSCdx84696)
- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Resolved Caveats in Cisco IOS Release 12.1(13)EW1

This section lists the resolved caveats in Release 12.1(13)EW1.

- Non-CDP phones (such as Softphone and VIP) that are connected to a Catalyst 4500 series switch running IOS are not discovered by Cisco Emergency Responder (CER).

  Workaround: None. (CSCin28373)
- When you run “snmpwalk” (or a similar tool) over dot1dTpFdbTable, the system might not report every other consecutive learned host.

  Workaround: Use the **show mac-address** command instead. (CSCdz72134)
- If you enter the **show interface capabilities** command on a Catalyst 4000 family switch running release 12.1(13)EW, the switch reloads unexpectedly; this command is not supported in the 12.1(13)EW release.

  Workaround: None. (CSCdz64100)
- If you have assigned a policer to a policy map, and if you have changed parameters such as rate and burst, the new parameters sometimes do not take effect.

  Workaround: After changing the parameters, first disable and enable global QoS, then disable and enable QoS on the port or VLAN that is using this policy map. (CSCdz75217)
- A Catalyst 4000 family switch might reset itself when you enable a VMPS client as well as multiple ports (for dynamic VLAN assignment).

  Workaround: None. (CSCdz80184)
- A Catalyst 4000 family switch with Supervisor Engine III or IV running release 12.1(12c)EW1 might reload due to an exception on the tcp_putbyte process.

  Workaround: None. (CSCdz69546)
- Policy-based routing (PBR) causes your Catalyst 4000 family switch to shut down when running release 12.1(13)EW.

  Workaround: None. (CSCdz89145)
- When a large number of flows use a congested queue, some non aggressive flows might experience large drops of traffic. When the queue is cleared, the packets flow normally for all the flows.

  Workaround: None. (CSCea19319)

Open Caveats in Cisco IOS Release 12.1(13)EW

This section lists the open caveats in Release 12.1(13)EW.

- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Workaround: Cisco has made software available, free of charge, to correct the problem. (CSCdz71127)

  This advisory is available at this URL:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030717-blocked

- Under certain conditions, a caveat in the power on self test (POST) may erroneously indicate that good WS-X4014 and WS-X4515 supervisor engines are faulty. When this happens, modules do not come online and the switch cannot be used to forward traffic.

  If the POST incorrectly identifies a good supervisor engine as faulty because of this situation, the POST output will only display the first port on the switch as faulty:

  ```
  Port Traffic: L2 Serdes Loopback ...
  0: F  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
  12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
  24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: .
  ```

  If the POST fails, but the test output does not match the display shown here, your hardware probably is faulty.

  This POST behavior is a software issue and has been resolved in 12.1(12c)EW2, 12.1(13)EW2, 12.1(19)EW, and 12.1(20)E images.

  Workaround: None. (CSCeb59442)

- When oversubscribed traffic destined for queue 4 is dropped in queue 4, the DBL drop counters for queue 2 (seen when the **show int <int> counter** command is issued) are incremented. When oversubscribed traffic destined for queue 2 is dropped in queue 2, the DBL drop counters for queue 4 are incremented.

  Queues 1 and 3 perform correctly.

  Workaround: None. (CSCdz58560)

- When IGMP Snooping is enabled and the last member leaves a multicast group, the switch will send an IGMP leave message with the source IP address of 0.0.0.0.

  Workaround: None. (CSCdz49171)

- Supervisor engine status may not register as faulty and the status LED may not turn amber when a fan-tray fails or is removed. Moreover, the status LED may not go turn red when the power supply fails or is removed.

  Workaround: None. (CSCdz55274)

- When a non-blocking gigaport is configured as “unidirectional receive-only” as well as “speed nonegotiation,” once both CLIs are unconfigured, the port link may not come up.

Workaround: Do one of the following:

- Avoid configuring both unidirectional receive-only and speed nonegotiation on the same port, because the former places a port in speed nonegotiation mode.
- Issue **shut** and **no shut** commands to reset the port's link partner and bring up the port's link. (CSCdz53781)

- When the fan tray is removed from the switch for more than 5 minutes, the following message is displayed on the console and all line cards are reset:

```
%C4K_CHASSIS-2-INSUFFICIENTFANSDETECTED: Too few working fans, the chassis will
overheat
```

  Workaround: None. (CSCdz50817)

- When a Catalyst 4000 Supervisor Engine III or IV is configured to use PBR, and the route-map specifies that the action is a default next-hop, that action is taken only if the ARP resolution for the specified host has already taken place. If the ARP resolution has not taken place, the system does not consider the host to be a valid default next-hop.

  Workaround: Ping the specified host to ensure that it is always in the ARP table. (CSCdz50786)

- If none of a port-channel's ports support Jumbo Frame, your attempt to change the MTU on the port-channel will change the port-channel's MTU, but not the member ports' MTU. Moreover, none of the member ports are suspended.

  In contrast, if some of the member ports support jumbo frames, this scenario does not happen and the ports that don't support jumbo frames are suspended.

  Workaround: Do not change the port-channel's MTU if none of its member ports support jumbo frames. (CSCdz43350)

- When PBR is configured on a Catalyst 4000 Supervisor Engine III or IV, PBR packets switched by hardware update the access-list or route-map statistics improperly.

  Workaround: None. (CSCdz10171)

- When the WS-X4148-RJ45V card is plugged into a Catalyst 4500 chassis, the power LED "on" does not work. This caveat is present in 12.1(13)EW and all previous software releases.

  Workaround: None. (CSCdz60995)

- With at least 2000 VLAN interfaces configured in the startup-config file, a switch might take at least 10 minutes to boot up. During this time, the switch is unresponsive.

  Workaround: Configure fewer SVIs in the startup config file. (CSCdx91258)

- Disabling IGMP snooping with a large number of groups and VLANs might cause CPU HOG and HOST FLAPPING. If so, you will see messages like the following on the console:

```
%SYS-3-CPUHOG: Task ran for 8692 msec (0/0), process = Exec, PC = 128790.
%C4K_EBM-4-HOSTFLAPPING: Host 00:10:0B:10:B9:20 in vlan 200 is flapping between port
Po2 and port Po1
```

  Workaround: None. (CSCdy21031)

- When the spanning tree mode is PVST, isolated trunk ports transmit BPDUs with the primary VLAN instead of the secondary VLAN.

  Workaround: Use the **spanning-tree bpduguard enable** interface command to enable BPDU Guard to detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the **shutdown** VLAN configuration command and re-enabled using the **no shutdown** VLAN configuration command, any subsequent flooded/multicast packets received on the private VLAN port does not reach all the destinations.

  Workaround: Do not use the **shutdown** and **no shutdown** VLAN configuration command to disable the VLAN. Instead, delete and recreate the secondary VLAN with the proper VLAN type and association configuration. (CSCdy22082)

- When a VLAN filter is applied to filter IP traffic based on Layer 4 information, fragmented packets might not be filtered correctly. Only the initial fragment has all the Layer 4 information. Non-initial fragments do not have any Layer 4 information (e.g., UDP ports, TCP flag, etc.).

  Workaround: If IP packets can be fragmented in your network, program ACLs in the VLAN Map, without any Layer 4 information. (CSCdx84696)

- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Resolved Caveats in Cisco IOS Release 12.1(13)EW

This section lists the resolved caveats in Release 12.1(13)EW.

- Private VLAN trunks will continue to operate as private trunks after you configure them as normal trunks using the **switchport mode trunk** command. While the trunks are in this state, the interfaces will not show up as private VLAN trunks in the output of the **show vlan private-vlan** command.

  Workaround: To ensure that the ports operate as normal trunks, issue shutdown/no shutdown commands after configuring the ports as normal trunks. (CSCdy40311)

- On systems with redundant supervisors and large and complex configurations, where the system is actively processing startup-config file, the standby supervisor engine may take over from the active supervisor engine in the boot process. If this happens, the following message is displayed on the active supervisor:

  ```
  C4K_REDUNDANCY-4-CONFIGSYNCFAIL: Persistent-config Sync to Standby Supervisor failed
  ```

  and the following messages display on the standby supervisor:

  ```
  C4k_REDUNDANCY-6-SWITCHOVER: Switchover activity detected, changing role from STANDBY
  to ACTIVE
  C4K_REDUNDANCY-6-INIT: Initializing as ACTIVE supervisor
  ```

  Workaround: Keep your startup-config file reasonably small size. (CSCdy02031)

- The CLI erroneously permits enabling 802.1X on ports that are configured as private VLAN trunks and private VLAN access ports. This configuration may cause unexpected behavior.

  Workaround: Don't configure 802.1X on PVLAN ports. (CSCdy23098)

Open Caveats in Cisco IOS Release 12.1(12c)EW4

This section lists the open caveats in release 12.1(12c)EW4.

- Private VLAN trunks will continue to operate as private trunks after you configure them as normal trunks using the **switchport mode trunk** command. While the trunks are in this state, the interfaces will not show up as private VLAN trunks in the output of the **show vlan private-vlan** command.

  Workaround: To ensure that the ports operate as normal trunks, issue shutdown/no shutdown commands after configuring the ports as normal trunks. (CSCdy40311)

- With approximately 2000 or more VLAN interfaces configured in the startup-config file, the switch might take at least 10 minutes to boot up. The switch is unresponsive until it completes the boot.

  Workaround: Configure fewer SVIs in the startup config file. (CSCdx91258)

- Disabling IGMP snooping with a large number of groups and VLANs might cause CPU HOG and HOST FLAPPING. If so, you will see messages like the following on the console:

  ```
  2d07h: %SYS-3-CPUHOG: Task ran for 8692 msec (0/0), process = Exec, PC = 128790.
  2d07h: %C4K_EBM-4-HOSTFLAPPING: Host 00:10:0B:10:B9:20 in vlan 200 is flapping between
  port Po2 and port Po1
  ```

  Workaround: None. (CSCdy21031)

- When the spanning tree mode is PVST, isolated trunk ports transmit BPDUs with the primary VLAN instead of the secondary VLAN.

  Workaround: Use the **spanning-tree bpduguard enable** interface command to enable BPDU Guard to detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the **shutdown** VLAN configuration command and re-enabled using the **no shutdown** VLAN configuration command, any subsequent flooded/multicast packets received on the private VLAN port do not reach all the destinations.

  Workaround: Do not use the **shutdown** and **no shutdown** VLAN configuration command to disable the VLAN. Instead, delete and recreate the secondary VLAN with the proper VLAN type and association configuration. (CSCdy22082)

- When a VLAN filter is applied to filter IP traffic based on Layer 4 information, fragmented packets might not be filtered correctly. Only the initial fragment has all the Layer 4 information. Non-initial fragments do not have any Layer 4 information (e.g.: UDP ports, TCP flag, etc.).

  Workaround: If IP packets can be fragmented in your network, program ACLs in the VLAN Map, without any Layer 4 information. (CSCdx84696)

- On systems with redundant supervisors and large and complex configurations, where the system is actively processing startup-config file, the standby supervisor engine may take over from the active supervisor engine in the boot process. If this happens, the following message displays on the active supervisor”

  ```
  C4K_REDUNDANCY-4-CONFIGSYNCFAIL: Persistent-config Sync to Standby Supervisor failed
  ```

  and the following messages display on the standby supervisor:

  ```
  C4k_REDUNDANCY-6-SWITCHOVER: Switchover activity detected, changing role from STANDBY
  to ACTIVE
  C4K_REDUNDANCY-6-INIT: Initializing as ACTIVE supervisor
  ```

  Workaround: Keep your startup-config file reasonably small. (CSCdy02031)

- The CLI erroneously permits enabling 802.1X on ports that are configured as private VLAN trunks and private VLAN access ports. This configuration may result in unexpected behavior.

  Workaround: Don't configure 802.1X on PVLAN ports. (CSCdy23098)

- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Resolved Caveats in Cisco IOS Release 12.1(12c)EW4

This section lists the resolved caveats in Release 12.1(12c)EW4.

- Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability. (CSCei76358)

- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  (CSCei61732)

Open Caveats in Cisco IOS Release 12.1(12c)EW3

This section lists the open caveats in release 12.1(12c)EW3.

- Private VLAN trunks will continue to operate as private trunks after you configure them as normal trunks using the **switchport mode trunk** command. While the trunks are in this state, the interfaces will not show up as private VLAN trunks in the output of the **show vlan private-vlan** command.

  Workaround: To ensure that the ports operate as normal trunks, issue shutdown/no shutdown commands after configuring the ports as normal trunks. (CSCdy40311)

- With approximately 2000 or more VLAN interfaces configured in the startup-config file, the switch might take at least 10 minutes to boot up. The switch is unresponsive until it completes the boot.

  Workaround: Configure fewer SVIs in the startup config file. (CSCdx91258)

- Disabling IGMP snooping with a large number of groups and VLANs might cause CPU HOG and HOST FLAPPING. If so, you will see messages like the following on the console:

  ```
  2d07h: %SYS-3-CPUHOG: Task ran for 8692 msec (0/0), process = Exec, PC = 128790.
  2d07h: %C4K_EBM-4-HOSTFLAPPING: Host 00:10:0B:10:B9:20 in vlan 200 is flapping between
  port Po2 and port Po1
  ```

  Workaround: None. (CSCdy21031)

- When the spanning tree mode is PVST, isolated trunk ports transmit BPDUs with the primary VLAN instead of the secondary VLAN.

  Workaround: Use the **spanning-tree bpduguard enable** interface command to enable BPDU Guard to detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the **shutdown** VLAN configuration command and re-enabled using the **no shutdown** VLAN configuration command, any subsequent flooded/multicast packets received on the private VLAN port do not reach all the destinations.

  Workaround: Do not use the **shutdown** and **no shutdown** VLAN configuration command to disable the VLAN. Instead, delete and recreate the secondary VLAN with the proper VLAN type and association configuration. (CSCdy22082)

- When a VLAN filter is applied to filter IP traffic based on Layer 4 information, fragmented packets might not be filtered correctly. Only the initial fragment has all the Layer 4 information. Non-initial fragments do not have any Layer 4 information (e.g.: UDP ports, TCP flag, etc.).

  Workaround: If IP packets can be fragmented in your network, program ACLs in the VLAN Map, without any Layer 4 information. (CSCdx84696)

- On systems with redundant supervisors and large and complex configurations, where the system is actively processing startup-config file, the standby supervisor engine may take over from the active supervisor engine in the boot process. If this happens, the following message displays on the active supervisor”

  ```
  C4K_REDUNDANCY-4-CONFIGSYNCFAIL: Persistent-config Sync to Standby Supervisor failed
  ```

  and the following messages display on the standby supervisor:

  ```
  C4k_REDUNDANCY-6-SWITCHOVER: Switchover activity detected, changing role from STANDBY
  to ACTIVE
  C4K_REDUNDANCY-6-INIT: Initializing as ACTIVE supervisor
  ```

  Workaround: Keep your startup-config file reasonably small. (CSCdy02031)

- The CLI erroneously permits enabling 802.1X on ports that are configured as private VLAN trunks and private VLAN access ports. This configuration may result in unexpected behavior.

  Workaround: Don't configure 802.1X on PVLAN ports. (CSCdy23098)

- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Resolved Caveats in Cisco IOS Release 12.1(12c)EW3

This section lists the resolved caveats in Release 12.1(12c)EW3.

- NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

  ```
  cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
  cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
  cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
  ```

```
cnfFeatureActiveSlot         1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable              1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry              1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType               1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot               1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive             1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches           1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches           1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges      1.3.6.1.4.1.9.9.99999.1.3.4.1.6
```

(CSCsa81379)

Open Caveats in Cisco IOS Release 12.1(12c)EW2

This section lists the open caveats in release 12.1(12c)EW2.

- Private VLAN trunks will continue to operate as private trunks after you configure them as normal trunks using the **switchport mode trunk** command. While the trunks are in this state, the interfaces will not show up as private VLAN trunks in the output of the **show vlan private-vlan** command.

  Workaround: To ensure that the ports operate as normal trunks, issue shutdown/no shutdown commands after configuring the ports as normal trunks. (CSCdy40311)

- With approximately 2000 or more VLAN interfaces configured in the startup-config file, the switch might take at least 10 minutes to boot up. The switch is unresponsive until it completes the boot.

  Workaround: Configure fewer SVIs in the startup config file. (CSCdx91258)

- Disabling IGMP snooping with a large number of groups and VLANs might cause CPU HOG and HOST FLAPPING. If so, you will see messages like the following on the console:

  ```
  2d07h: %SYS-3-CPUHOG: Task ran for 8692 msec (0/0), process = Exec, PC = 128790.
  2d07h: %C4K_EBM-4-HOSTFLAPPING: Host 00:10:0B:10:B9:20 in vlan 200 is flapping between
  port Po2 and port Po1
  ```

  Workaround: None. (CSCdy21031)

- When the spanning tree mode is PVST, isolated trunk ports transmit BPDUs with the primary VLAN instead of the secondary VLAN.

  Workaround: Use the **spanning-tree bpduguard enable** interface command to enable BPDU Guard to detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the **shutdown** VLAN configuration command and re-enabled using the **no shutdown** VLAN configuration command, any subsequent flooded/multicast packets received on the private VLAN port do not reach all the destinations.

  Workaround: Do not use the **shutdown** and **no shutdown** VLAN configuration command to disable the VLAN. Instead, delete and recreate the secondary VLAN with the proper VLAN type and association configuration. (CSCdy22082)

- When a VLAN filter is applied to filter IP traffic based on Layer 4 information, fragmented packets might not be filtered correctly. Only the initial fragment has all the Layer 4 information. Non-initial fragments do not have any Layer 4 information (e.g.: UDP ports, TCP flag, etc.).

  Workaround: If IP packets can be fragmented in your network, program ACLs in the VLAN Map, without any Layer 4 information. (CSCdx84696)

- On systems with redundant supervisors and large and complex configurations, where the system is actively processing startup-config file, the standby supervisor engine may take over from the active supervisor engine in the boot process. If this happens, the following message displays on the active supervisor”

  ```
  C4K_REDUNDANCY-4-CONFIGSYNCFAIL: Persistent-config Sync to Standby Supervisor failed
  ```

  and the following messages display on the standby supervisor:

  ```
  C4k_REDUNDANCY-6-SWITCHOVER: Switchover activity detected, changing role from STANDBY
  to ACTIVE
  C4K_REDUNDANCY-6-INIT: Initializing as ACTIVE supervisor
  ```

  Workaround: Keep your startup-config file reasonably small. (CSCdy02031)

- The CLI erroneously permits enabling 802.1X on ports that are configured as private VLAN trunks and private VLAN access ports. This configuration may result in unexpected behavior.

  Workaround: Don't configure 802.1X on PVLAN ports. (CSCdy23098)

- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Resolved Caveats in Cisco IOS Release 12.1(12c)EW2

This section lists the resolved caveats in Release 12.1(12c)EW2.

- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Workaround: Cisco has made software available, free of charge, to correct the problem. (CSCdz71127, CSCea02355)

  This advisory is available at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030717-blocked

- Under certain conditions, a caveat in the power on self test (POST) may erroneously indicate that good WS-X4014 and WS-X4515 supervisor engines are faulty. When this happens, modules do not come online and the switch cannot be used to forward traffic.

  If the POST incorrectly identifies a good supervisor engine as faulty because of this situation, the POST output will only display the first port on the switch as faulty:

  ```
  Port Traffic: L2 Serdes Loopback ...
  0: F  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
  12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
  24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: .
  ```

  If the POST fails, but the test output does not match the display shown here, your hardware probably is faulty.

This POST behavior is a software issue and has been resolved in 12.1(12c)EW2, 12.1(13)EW2, 12.1(19)EW, and 12.1(20)E images.

Workaround: None. (CSCeb59442)

Open Caveats in Cisco IOS Release 12.1(12c)EW1

This section lists the open caveats in Release 12.1(12c)EW1.

- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Workaround: Cisco has made software available, free of charge, to correct the problem. (CSCdz71127, CSCea02355)

  This advisory is available at this URL:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030717-blocked

- Under certain conditions, a caveat in the power on self test (POST) may erroneously indicate that good WS-X4014 and WS-X4515 supervisor engines are faulty. When this happens, modules do not come online and the switch cannot be used to forward traffic.

  If the POST incorrectly identifies a good supervisor engine as faulty because of this situation, the POST output will only display the first port on the switch as faulty:

  ```
  Port Traffic: L2 Serdes Loopback ...
  0: F  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
  12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
  24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: .
  ```

  If the POST fails, but the test output does not match the display shown here, your hardware probably is faulty.

  This POST behavior is a software issue and has been resolved in 12.1(12c)EW2, 12.1(13)EW2, 12.1(19)EW, and 12.1(20)E images.

  Workaround: None. (CSCeb59442)

- Private VLAN trunks will continue to operate as private trunks after you configure them as normal trunks using the **switchport mode trunk** command. While the trunks are in this state, the interfaces will not show up as private VLAN trunks in the output of the **show vlan private-vlan** command.

  Workaround: To ensure that the ports operate as normal trunks, issue shutdown/no shutdown commands after configuring the ports as normal trunks. (CSCdy40311)

- With approximately 2000 or more VLAN interfaces configured in the startup-config file, the switch might take at least 10 minutes to boot up. The switch is unresponsive until it completes the boot.

  Workaround: Configure fewer SVIs in the startup config file. (CSCdx91258)

- Disabling IGMP snooping with a large number of groups and VLANs might cause CPU HOG and HOST FLAPPING. If so, you will see messages like the following on the console:

  ```
  2d07h: %SYS-3-CPUHOG: Task ran for 8692 msec (0/0), process = Exec, PC = 128790.
  2d07h: %C4K_EBM-4-HOSTFLAPPING: Host 00:10:0B:10:B9:20 in vlan 200 is flapping between
  port Po2 and port Po1
  ```

Workaround: None. (CSCdy21031)

- When the spanning tree mode is PVST, isolated trunk ports transmit BPDUs with the primary VLAN instead of the secondary VLAN.

  Workaround: Use the **spanning-tree bpduguard enable** interface command to enable BPDU Guard to detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the **shutdown** VLAN configuration command and re-enabled using the **no shutdown** VLAN configuration command, any subsequent flooded/multicast packets received on the private VLAN port do not reach all the destinations.

  Workaround: Do not use the **shutdown** and **no shutdown** VLAN configuration command to disable the VLAN. Instead, delete and recreate the secondary VLAN with the proper VLAN type and association configuration. (CSCdy22082)

- When a VLAN filter is applied to filter IP traffic based on Layer 4 information, fragmented packets might not be filtered correctly. Only the initial fragment has all the Layer 4 information. Non-initial fragments do not have any Layer 4 information (e.g.: UDP ports, TCP flag, etc.).

  Workaround: If IP packets can be fragmented in your network, program ACLs in the VLAN Map, without any Layer 4 information. (CSCdx84696)

- On systems with redundant supervisors and large and complex configurations, where the system is actively processing startup-config file, the standby supervisor engine may take over from the active supervisor engine in the boot process. If this happens, the following message displays on the active supervisor"

  ```
  C4K_REDUNDANCY-4-CONFIGSYNCFAIL: Persistent-config Sync to Standby Supervisor failed
  ```

  and the following messages display on the standby supervisor:

  ```
  C4k_REDUNDANCY-6-SWITCHOVER: Switchover activity detected, changing role from STANDBY
  to ACTIVE
  C4K_REDUNDANCY-6-INIT: Initializing as ACTIVE supervisor
  ```

  Workaround: Keep your startup-config file reasonably small. (CSCdy02031)

- The CLI erroneously permits enabling 802.1X on ports that are configured as private VLAN trunks and private VLAN access ports. This configuration may result in unexpected behavior.

  Workaround: Don't configure 802.1X on PVLAN ports. (CSCdy23098)

- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Resolved Caveats in Cisco IOS Release 12.1(12c)EW1

This section lists the resolved caveats in Release 12.1(12c)EW1:

- On a 4507R chassis with dual supervisors, the following message displays during switchover under high CPU utilization:

  ```
  %Error: Opening vlan.dat on STANDBY
  ```

Workaround: After the switch boots, verify that the standby supervisor engine has a valid cat4000_flash:vlan.dat file. If you suspect the file is invalid, copy the valid file using the following command on the active supervisor:

copy cat4000_flash:vlan.dat slavecat4000_flash:vlan.dat

(CSCdy26890)

- No log message is generated when a power supply fails.

  Workaround:.Review the output of the **show power** command to check the status of power supplies. This is the only way to be notified of a supply failure. (CSCdy33518)

- When DHCP snooping, DHCP relay agent and CEF are all enabled on a switch, a DHCP server reply packet that is destined for the DHCP relay agent might get forwarded to the DHCP client.

  Workaround: Either not enable all these features at the same time, or upgrade the switch to the latest maintenance release image that contains the fix for this problem.

- A Catalyst 4000 supervisor engine running 12.1(12c)EW or an earlier release will not link up on a WS-X4424-GB-RJ45 line card interface if it is hard-coded for speed and duplex.

  Workaround: Issue a shutdown/ no shutdown command at the associated interface to bring up the link.

  When you force the speed, the switch port does not auto-detect crossover/straight through cables. In these situations, you must use the correct cable.

  - When connecting the switch port to another networking device, use a crossover cable.
  - When connecting the switch port to a workstation, use a straight through cable. (CSCdy44221)

- When the tcam entries in the ingress VLAN are exhausted, and when DHCP snooping is enabled in the VLAN, the packets that are punted to software for ACL processing might bypass the router ACLs.

  Workaround: None. (CSCdy47753)

- DHCP packets that are relayed by DHCP Relay Agents are treated as IOS internally-generated packets. This means that the output router ACL won't apply to these packets.

  Workaround: Apply an input router ACL to filter out those broadcast DHCP packets before they can be relayed by the Agent. (CSCdy50604)

- DHCP broadcast requests from a DHCP client will bypass router ACLs when DHCP snooping is disabled on the switch.

  Workaround: Either enable the DHCP snooping feature, or use a VACL instead of a router ACL to filter the DHCP packets. (CSCdy62123)

- When you boot diskless-workstations remotely, you might experience slow booting on random ports of the WS-X-4148-RJ45V module when used in conjunction with the Supervisor Engine III.

  Workaround: First, change the duplex to half, then reconfigure to full. (CSCdy67241)

- Under certain conditions, if numerous ACLs are configured on boot-up, some ACLs or QoS policies will not be programmed in the hardware and the following error messages will display:

```
*Sep 19 21:53:17.947: %C4K_HWACLMAN-4-ACLHWPROGERR: <Feature using ACLs>- hardware
TCAM limit, ...
*Sep 19 21:53:17.975: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: <Feature using ACLs>- out of
software acl programming resources.
```

  Workaround: Re-apply the ACLs to the appropriate security ACL or QoS policy-map. (CSCdy68681)

- ACLs containing more than six L4 port operators trigger L4 operator expansion. Certain range operators are expanded too broadly, which causes the affected ACEs to match more packets than they should. Less-than and greater-than operators are expanded correctly in all cases. This issue affects only Cisco IOS Release 12.1(12c)EW.

  Workaround: Avoid configuring ACLs that trigger L4 operator expansion. (CSCdy70646)

Open Caveats in Cisco IOS Release 12.1(12c)EW

This section lists the open caveats in Release 12.1(12c)EW.

- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Workaround: Cisco has made software available, free of charge, to correct the problem. (CSCdz71127, CSCea02355)

  This advisory is available at this URL:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030717-blocked

- Under certain conditions, a caveat in the power on self test (POST) may erroneously indicate that good WS-X4014 and WS-X4515 supervisor engines are faulty. When this happens, modules do not come online and the switch cannot be used to forward traffic.

  If the POST incorrectly identifies a good supervisor engine as faulty because of this situation, the POST output will only display the first port on the switch as faulty:

  ```
  Port Traffic: L2 Serdes Loopback ...
  0: F  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
  12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
  24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: .
  ```

  If the POST fails, but the test output does not match the display shown here, your hardware probably is faulty.

  This POST behavior is a software issue and has been resolved in 12.1(12c)EW2, 12.1(13)EW2, 12.1(19)EW, and 12.1(20)E images.

  Workaround: None. (CSCeb59442)

- Private VLAN trunks will continue to operate as private trunks after you configure them as normal trunks using the **switchport mode trunk** command. While the trunks are in this state, the interfaces will not show up as private VLAN trunks in the output of the **show vlan private-vlan** command.

  Workaround: To ensure that the ports operate as normal trunks, issue shutdown/no shutdown commands after configuring the ports as normal trunks. (CSCdy40311)

- With approximately 2000 or more VLAN interfaces configured in the startup-config, the switch might take at least 10 minutes to boot up. The switch is unresponsive until it completes the boot.

  Workaround: Configure fewer SVIs in the startup config. (CSCdx91258)

- Disabling IGMP snooping with a large number of groups and VLANs might cause CPU HOG and HOST FLAPPING. If so, you will see messages like the following on the console:

  ```
  2d07h: %SYS-3-CPUHOG: Task ran for 8692 msec (0/0), process = Exec, PC = 128790.
  2d07h: %C4K_EBM-4-HOSTFLAPPING: Host 00:10:0B:10:B9:20 in vlan 200 is flapping between
  port Po2 and port Po1
  ```

  Workaround: None. (CSCdy21031)

- When the spanning tree mode is PVST, isolated trunk ports transmit BPDUs with the primary VLAN instead of the secondary VLAN.

  Workaround: Use the **spanning-tree bpduguard enable** interface command to enable BPDU Guard to detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the **shutdown** VLAN configuration command and re-enabled using the **no shutdown** VLAN configuration command, any subsequent flooded/multicast packets received on the private VLAN port does not reach all the destinations.

  Workaround: If possible, do not use the **shutdown** and **no shutdown** VLAN configuration command to disable the VLAN. Instead, delete and recreate the secondary VLAN with the proper VLAN type and association configuration. (CSCdy22082)

- When a VLAN filter is applied to filter IP traffic based on Layer 4 information, fragmented packets may not be filtered correctly. Only the initial fragment has all the Layer 4 information. Non-initial fragments do not have any Layer 4 information (e.g.: UDP ports, TCP flag, etc.).

  Workaround: If IP packets can be fragmented in your network, program ACLs in the VLAN Map, without any Layer 4 information. (CSCdx84696)

- On systems with redundant supervisors and large and complex configurations, where the system is actively processing startup-config, the standby supervisor engine may take over from the active supervisor engine in the boot process. If this happens, the following message displays on the active supervisor:

  ```
  C4K_REDUNDANCY-4-CONFIGSYNCFAIL: Persistent-config Sync to Standby Supervisor failed
  ```

  and the following messages display on the standby supervisor

  ```
  C4k_REDUNDANCY-6-SWITCHOVER: Switchover activity detected, changing role from STANDBY
  to ACTIVE
  C4K_REDUNDANCY-6-INIT: Initializing as ACTIVE supervisor
  ```

  Workaround: Keep your startup-config reasonably small. (CSCdy02031)

- The CLI erroneously permits enabling 802.1X on ports that are configured as private VLAN trunks and private VLAN access ports. This configuration may result in unexpected behavior.

  Workaround: Don't configure 802.1X on PVLAN ports. (CSCdy23098)

- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Resolved Caveats in Cisco IOS Release 12.1(12c)EW

This section lists the resolved caveats in Release 12.1(12c)EW:

- A Catalyst 4006 switch with Supervisor Engine III using Release 12.1(11b)EW might crash when you enter the following command while the port channel set to **channel-no** is in a shutdown state:

  show platform software etherchannel port-channel channel-no

  This command was introduced in software release 12.1(11b)EW. Software release 12.1(8a)EW is not affected by this caveat.

  Workaround: Do not use the above command for a port channel in a shutdown state. (CSCdx47694)
- On a Catalyst 4006 switch with Supervisor Engine III, the output rate in **show interface** command might display a value greater than the bandwidth that the interface can handle. There is no workaround. (CSCdx30670)
- When you use a large number of ACLs with more than 1000 entries each, the switch boot up time will be extended.

  Workaround: Use extended named ACLs. Named ACLs specified in the ACL config mode do not exhibit this behavior. (CSCdw20032)
- A Cisco router configured for Multicast Source Discovery Protocol (MSDP) can experience frequent MSDP session resets with the MSDP peers of the router. This situation is often caused by excessive Source, Group (S, G) information that should be contained in a domain being passed to the outside, resulting in additional entries in the Source-Active (SA) cache.

  Workarounds: Determine whether the routers have the SA filters configured properly by reviewing the MSDP SA filter recommendations posted at the following URL: ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt

  Determine whether the router is running a Cisco IOS image that has the correction for CSCdr93446 (MSDP: Reducing SA storms and session resets (MSDP rearchitect)).

  Review the output of the **show ip msdp sa-cache** EXEC command to see if some of the SAs can be filtered based on the source address, the Rendezvous point (RP) address, or the autonomous system (AS) number. (CSCdw35003)
- If you configure "inst 1 vlan 1," topology change BPDUs are sent for 35 second rather than 2* hello time in the MST neighbor. There is no workaround. (CSCdy30488)

Open Caveats in Cisco IOS Release 12.1(11b)EW1

This section lists the open caveats in Release 12.1(11b)EW1:

- If you configure "inst 1 vlan 1," typology change BPDUs are sent for 35 second rather than 2* hello time in the MST neighbor. There is no workaround. (CSCdy30488)
- A Catalyst 4006 switch with Supervisor Engine III using Release 12.1(11b)EW might crash when you enter the following command while the port channel set to **channel-no** is in a shutdown state:

  show platform software etherchannel port-channel channel-no

  This command was introduced in software release 12.1(11b)EW. Software release 12.1(8b)EW is not affected by this caveat.

  Workaround: Do not use the above command for a port channel in a shutdown state. (CSCdx47694)

- On a Catalyst 4006 switch with Supervisor Engine III, the output rate in **show interface** command might display a value greater than the bandwidth that the interface can handle.

  Workaround: None. (CSCdx30670)
- When you use a large number of ACLs with more than 1000 entries, the switch can take more than five minutes to boot up.

  Workaround: Use extended named ACLs. Named ACLs specified in the ACL config mode do not exhibit this behavior. (CSCdw20032)
- Under some conditions, the following error message will appear:

  ```
  3d03h: %FIB-4-FIBIDB: Missing cef idb for GigabitEthernet2/6 during address ch
  ```

  When this happens, traffic to or from that interface will not be received or forwarded correctly.

  Workaround: Functionality might be restored by bringing the interface administratively down and up, or by disabling and re-enabling IP routing. (CSCdx37609)
- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Resolved Caveats in Cisco IOS Release 12.1(11b)EW1

This section lists the resolved caveats in Release 12.1(11b)EW1:

- Under some conditions, the Supervisor Engine III (WS-X4014) might stop switching traffic on all connected ports. Should this occur, all incoming data traffic will be dropped.

  When the switch enters this state, the NoPacketBuffAvailOrCdmFifoOverruns counter will increment on all ports that have received incoming data traffic. You can display the contents of the NoPacketBuffAvailOrCdmFifoOverruns counter by entering the **show platform software interface statistics** command.

  Workaround: This condition is temporary and can be resolved by resetting the switch. (CSCdx66345)
- When burst CPU traffic conditions (low CPU traffic combined with intermittent bursts of routing updates) occur, packets sent to the CPU can be lost. This traffic interruption can occur for less than one second or for a few minutes. No intervention is required, the switch recovers automatically. (CSCdy06162)

Open Caveats in Cisco IOS Release 12.1(11b)EW

This section lists the open caveats in Release 12.1(11b)EW:

- Under some conditions, the Supervisor Engine III (WS-X4014) might stop switching traffic on all connected ports. Should this occur, all incoming data traffic will be dropped.

  When the switch enters this state, the NoPacketBuffAvailOrCdmFifoOverruns counter will increment on all ports that have received incoming data traffic. You can display the contents of the NoPacketBuffAvailOrCdmFifoOverruns counter by entering the **show platform software interface statistics** command.

Workaround: This condition is temporary and can be resolved by resetting the switch. (CSCdx66345)

- When burst CPU traffic conditions (low CPU traffic combined with intermittent bursts of routing updates) occur, packets sent to the CPU can be lost. This traffic interruption can occur for less than one second or for a few minutes. No intervention is required, the switch recovers automatically. (CSCdy06162)
- A Catalyst 4006 switch with Supervisor Engine III using Release 12.1(11b)EW might crash when you enter the following command while the port channel set to **channel-no** is in a shutdown state:

  show platform software etherchannel port-channel channel-no

  This command was introduced in software release 12.1(11b)EW. Release 12.1(8b)EW is not affected by this caveat.

  Workaround: Do not use the above command for a port channel in a shutdown state. (CSCdx47694)
- On a Catalyst 4006 switch with Supervisor Engine III, the output rate in **show interface** command might display a value greater than the bandwidth that the interface can handle. There is no workaround. (CSCdx30670)
- When you use a large number of ACLs with more than 1000 entries, the switch can take more than five minutes to boot up.

  Workaround: Use extended named ACLs. Named ACLs specified in the ACL config mode do not exhibit this behavior. (CSCdw20032)
- Under some conditions, the following error message will appear:

  ```
  3d03h: %FIB-4-FIBIDB: Missing cef idb for GigabitEthernet2/6 during address ch
  ```

  When this happens, traffic to or from that interface will not be received or forwarded correctly.

  Workaround: Functionality might be restored by bringing the interface administratively down and up, or by disabling and re-enabling IP routing. (CSCdx37609)
- A Cisco router configured for Multicast Source Discovery Protocol (MSDP) can experience frequent MSDP session resets with the MSDP peers of the router. This situation is often caused by excessive Source, Group (S, G) information that should be contained in a domain being passed to the outside, resulting in additional entries in the Source-Active (SA) cache.

  Workarounds: Determine whether the routers have the SA filters configured properly by reviewing the MSDP SA filter recommendations posted at the following URL:
  ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt

  Determine whether the router is running a Cisco IOS image that has the correction for CSCdr93446 (MSDP: Reducing SA storms and session resets (MSDP rearchitect)).

  Review the output of the **show ip msdp sa-cache** EXEC command to see if some of the SAs can be filtered based on the source address, the Rendezvous point (RP) address, or the autonomous system (AS) number. (CSCdw35003)
- If an ACL is applied to more than one interface, and any Access Control Entry (ACE) in the ACL is subsequently modified, then the Ternary Content Addressable Memory (TCAM) usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: Detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

Resolved Caveats in Cisco IOS Release 12.1(11b)EW

This section lists the resolved caveats in Release 12.1(11b)EW:

- In the **show power** and **show environment** commands, the status of the Power Entry Module (PEM) is reported incorrectly. If the status of the PEM is listed as *bad*, it is actually good, and if the status is listed as *good,* it is actually bad. This has no affect on system operation. n software release 12.1(8a)EW1, the PEM is supported only in the **show** commands. (CSCdx05522)
- When a large number of ports (such as 240) have joined a large number of multicast groups, entering the **clear ip igmp group** command to delete IGMP group cache entries can sometimes reboot a Catalyst 4006 switch with Supervisor Engine III running Cisco IOS Release 12.1(8a)EW.

  Workaround: Do not clear the groups all at once. Instead, clear each IGMP group cache entry separately. (CSCdw46417)
- Occasionally, a switch may have errors when reading register status. When this occurs, the switch logs the message instead of recovering from the error by attempting to read the register status again. The hardware is not actually bad.There is no workaround. (CSCdx52952)
- Typing **Ctrl-/** when attached to the console port will cause the switch to reboot. There is no workaround. (CSCdw06454)
- If you create Switched Virtual Interfaces (SVI) for both a primary VLAN and secondary VLAN and then delete them, a subsequent association between the VLANs the switch could reboot your switch.

  Workaround: Don not create associations between VLANs if the SVI of the primary VLAN has been deleted. (CSCdw50014)
- Packets that are software-generated or software-forwarded are not transmitted in a SPAN session. This includes Layer 2 control packets, such as CDP or spanning tree BPDUs, and packets forwarded by software such as FIB, or adjacency overload scenarios. There is no workaround. (CSCdv34494)
- In an ACL, the **fragment** keyword is ignored when the protocol is **ip**. For all other protocols the keyword is applied to traffic as expected.

  Workaround: Replace the **permit ip any any fragment** command with the following commands:

  ```
  permit 1 any any fragment
  permit 2 any any fragment
  permit 255 any any fragment
  ```
  (CSCdw39872)
- The **show platform hardware monitor** command may corrupt the stack if it is invoked when a VSPAN session or a PSPAN session with many source interfaces is configured on the switch. There is no workaround; to be safe, do not use this command on switches running Cisco IOS Release 12.1(8a)EW. (CSCdw59733)

Open Caveats in Cisco IOS Release 12.1(8a)EW1

This section lists the open caveats in Release 12.1(8a)EW1:

- In the **show power** and **show environment** commands, the status of the Power Entry Module (PEM) is reported incorrectly. If the status of the PEM is listed as *bad*, it is actually good, and if the status is listed as *good,* it is actually bad. This has no affect on system operation. n software release 12.1(8a)EW1, the PEM is supported only in the **show** commands. (CSCdx05522)
- When a large number of ports (such as 240) have joined a large number of multicast groups, entering the **clear ip igmp group** command to delete IGMP group cache entries can sometimes reboot a Catalyst 4006 switch with Supervisor Engine III running Cisco IOS Release 12.1(8a)EW.

Workaround: Do not clear the groups all at once. Instead, clear each IGMP group cache entry separately. (CSCdw46417)

- When you use a large number of ACLs with more than 1000 entries, the switch can take more than five minutes to boot up.

  Workaround: Use extended named ACLs. Named ACLs specified in the ACL config mode do not exhibit this behavior. (CSCdw20032)

- A Cisco router configured for Multicast Source Discovery Protocol (MSDP) can experience frequent MSDP session resets with the MSDP peers of the router. This situation is often caused by excessive source, group (S, G) information that should be contained in a domain being passed to the outside, resulting in additional entries in the Source-Active (SA) cache.

  Workarounds: Determine if the routers have the SA filters configured properly by reviewing the MSDP SA filter recommendations posted at the following URL:
  ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt

  Determine if the router is running a Cisco IOS image that has the fix for CSCdr93446 (MSDP: Reducing SA storms and session resets (MSDP rearchitect)).

  Review the output of the **show ip msdp sa-cache** EXEC command to see if some of the SAs can be filtered based on the source address, the Rendezvous point (RP) address, or the autonomous system (AS) number. (CSCdw35003)

- Typing **Ctrl-/** when attached to the console port will cause the switch to reboot. There is no workaround. (CSCdw06454)

- If you create Switched Virtual Interfaces (SVI) for both a primary VLAN and secondary VLAN and then delete them, a subsequent association between the VLANs the switch could reboot your switch.

  Workaround: Don not create associations between VLANs if the SVI of the primary VLAN has been deleted. (CSCdw50014)

- In an ACL, the **fragment** keyword is ignored when the protocol is **ip**. For all other protocols the keyword is applied to traffic as expected.

  Workaround: Replace the **permit ip any any fragment** command with the following commands:

  ```
  permit 1 any any fragment
  permit 2 any any fragment
  permit 255 any any fragment
  ```
  (CSCdw39872)

- Packets that are software-generated or software-forwarded are not transmitted in a SPAN session. This includes Layer 2 control packets, such as CDP or spanning tree BPDUs, and packets forwarded by software such as FIB, or adjacency overload scenarios. There is no workaround. (CSCdv34494)

- If an ACL is applied to more than one interface, and any ACE in the ACL is subsequently modified, then the TCAM usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)

- The **show platform hardware monitor** command may corrupt the stack if it is invoked when a VSPAN session or a PSPAN session with many source interfaces is configured on the switch. There is no workaround; to be safe, do not use this command on switches running Cisco IOS Release 12.1(8a)EW. (CSCdw59733)

Resolved Caveats in Cisco IOS Release 12.1(8a)EW1

This section lists the resolved caveats in Release 12.1(8a)EW1:

- An error can occur with management protocol processing. Please use the following URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

  (CSCdw65903)

Open Caveats in Cisco IOS Release 12.1(8a)EW

This section lists the open caveats in Release 12.1(8a)EW:

- Under some conditions, the Supervisor Engine III (WS-X4014) might stop switching traffic on all connected ports. Should this occur, all incoming data traffic will be dropped.

  When the switch enters this state, the NoPacketBuffAvailOrCdmFifoOverruns counter will increment on all ports that have received incoming data traffic. You can display the contents of the NoPacketBuffAvailOrCdmFifoOverruns counter by entering the **show platform software interface statistics** command.

  Workaround: This condition is temporary and can be resolved by resetting the switch. (CSCdx66345)
- In the **show power** and **show environment** commands, the status of the Power Entry Module (PEM) is reported incorrectly. If the status of the PEM is listed as *bad*, it is actually good, and if the status is listed as *good,* it is actually bad. This has no affect on system operation. n software release 12.1(8a)EW1, the PEM is supported only in the **show** commands. (CSCdx05522)
- Typing **Ctrl-/** when attached to the console port will cause the switch to reboot. There is no workaround. (CSCdw06454)
- When a large number of ports (such as 240) have joined a large number of multicast groups, entering the **clear ip igmp group** command to delete IGMP group cache entries can sometimes reboot a Catalyst 4006 switch with Supervisor Engine III running Cisco IOS Release 12.1(8a)EW.

  Workaround: Do not clear the groups all at once. Instead, clear each IGMP group cache entry separately. (CSCdw46417)
- When you use a large number of ACLs with more than 1000 entries, the switch can take more than five minutes to boot up.

  Workaround: Use extended named ACLs. Named ACLs specified in the ACL config mode do not exhibit this behavior. (CSCdw20032)
- A Cisco router configured for Multicast Source Discovery Protocol (MSDP) can experience frequent MSDP session resets with the MSDP peers of the router. This situation is often caused by excessive source, group (S, G) information that should be contained in a domain being passed to the outside, resulting in additional entries in the Source-Active (SA) cache.

  Workarounds: Determine if the routers have the SA filters configured properly by reviewing the MSDP SA filter recommendations posted at the following URL: ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt

  Determine if the router is running a Cisco IOS image that has the fix for CSCdr93446 (MSDP: Reducing SA storms and session resets (MSDP rearchitect)).

Review the output of the **show ip msdp sa-cache** EXEC command to see if some of the SAs can be filtered based on the source address, the Rendezvous point (RP) address, or the autonomous system (AS) number. (CSCdw35003)

- If you create Switched Virtual Interfaces (SVI) for both a primary VLAN and secondary VLAN and then delete them, a subsequent association between the VLANs the switch could reboot your switch.

  Workaround: Don not create associations between VLANs if the SVI of the primary VLAN has been deleted. (CSCdw50014)
- If an ACL is applied to more than one interface, and any ACE in the ACL is subsequently modified, then the TCAM usage of that ACL is multiplied by the number of interfaces to which the ACL is applied.

  Workaround: detach the ACL from one interface at a time (without deleting the ACL), and then reattach the ACL to that interface. (CSCdw28603)
- In an ACL, the **fragment** keyword is ignored when the protocol is **ip**. For all other protocols the keyword is applied to traffic as expected.

  Workaround: Replace the **permit ip any any fragment** command with the following commands:

  ```
  permit 1 any any fragment
  permit 2 any any fragment
  permit 255 any any fragment
  ```
  (CSCdw39872)
- Packets that are software-generated or software-forwarded are not transmitted in a SPAN session. This includes Layer 2 control packets, such as CDP or spanning tree BPDUs, and packets forwarded by software such as FIB, or adjacency overload scenarios. There is no workaround. (CSCdv34494)
- The **show platform hardware monitor** command may corrupt the stack if it is invoked when a VSPAN session or a PSPAN session with many source interfaces is configured on the switch. There is no workaround; to be safe, do not use this command on switches running Cisco IOS Release 12.1(8a)EW. (CSCdw59733)

Resolved Caveats in Cisco IOS Release 12.1(8a)EW

There are no resolved caveats in software release 12.1(8a)EW.