Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Release 12.1(20)EW3

Current Release
12.1(20)EW3—May 11, 2005

Previous Releases
12.1(20)EW2, 12.1(20)EW1, 12.1(20)EW, 12.1(19)EW2, 12.1(19)EW1, 12.1(19)EW, 12.1(13)EW3, 12.1(13)EW1, 12.1(13)EW, 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:

- S4KL3-12120EW—Cisco IOS software for the Catalyst 4500 series, 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 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 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 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, 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 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 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)

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

- S4KL3EK2-12119EW—Cisco IOS software for the Catalyst 4500 series 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)
- FR-IRC4—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines III and IV with InterDomain Routing Feature License including BGP4
- S4KL3-12113EW—Cisco IOS software for the Catalyst 4500 Series 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 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 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 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 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 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

These release notes describe the features, modifications, and caveats for the Cisco IOS software on the Catalyst 4500 series switch. The most current software release is 12.1(20)EW.

Catalyst 4500 Series Switch Cisco IOS Software Release Strategy

This section describes the Catalyst 4500 series switch Cisco IOS release strategy for the Catalyst 4500 series Supervisor Engines II-Plus, Supervisor Engine III, Supervisor Engine IV,

Figure 1 shows the Catalyst 4500 series switch Cisco IOS software release strategy.

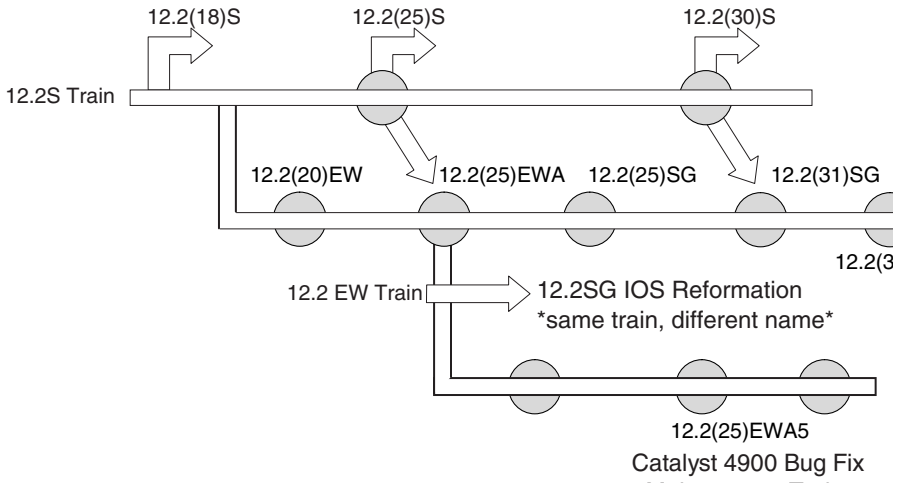
Cisco IOS Release 12.1(19)E1 contains only the software and hardware functionality up to and including Cisco IOS Release 12.1(12c)EW1. Subsequent releases on the 12.1 E train, including 12.1(20)E, will be maintenance releases with the Catalyst 4500 feature set in Release 12.1(12c)EW1 feature set. The 12.1 E train is on the General Deployment (GD) track. Cisco IOS software releases are on the 12.1 E train for

Catalyst 4500 series switch customers who require the stability of a GD release with a fixed set of features. Cisco IOS releases on the 12.1 E train are not available to Catalyst 4500 series switch Supervisor Engines II-Plus.

Beginning with Release 12.1(13)EW, additional software features and hardware support are introduced in the Cisco IOS 12.1 EW release train for the Catalyst 4500 series switch. Software features such as PBR, DBL, Port Security, and Jumbo Frames, as well as support for the Catalyst 4500 series switch NetFlow Services Card, Supervisor Engine II-Plus, 1000BaseT GBIC, and the AGM module are contained in the 12.1 EW release train. On the 12.1 EW train, the Catalyst 4500 series switch Supervisor Engine II-Plus is supported only in Release 12.1(19)EW and Release 12.1(20)EW. The latest Catalyst 4500 series switch Cisco IOS software release in the 12.1 EW train is Release 12.1(20)EW.

Starting with Release 12.2(18)EW, additional software features and hardware support are introduced in the 12.2 EW release train of Cisco IOS software for the Catalyst 4500 series switch. Software features such as sticky port security, 802.1X accounting, SmartPort macros, as well as support for the Catalyst 4510R chassis, the the IEEE Power over Ethernet (PoE) line cards are contained in the 12.2 EW release train. The Catalyst 4500 series switch Cisco IOS software in the 12.2 EW release train will continue to offer the latest hardware and software features. The 12.2 S mainline releases will be offered in the future to Catalyst 4500 series switch customers for feature consistency across the Catalyst platforms.

Figure 1 Software Release Strategy



Catalyst 4500 Series Switch Cisco IOS Software Release Migration Paths

Cisco IOS Software Release 12.2EW train offers the latest features for the Cisco Catalyst 4500 Series supervisor engines. Customers with Cisco Catalyst 4500 Series supervisor engines who need the latest hardware support and software features should migrate to Cisco IOS Software Release 12.2(25)EWA.

Cisco IOS Software Release 12.2(18)EW1 and all subsequent 12.2(18)EW maintenance releases have only the feature set based on Cisco IOS Software Release 12.2(18)EW for the Cisco Catalyst 4500 Series supervisor engines. Customers with Catalyst 4500 Series supervisor engines who require the stability of a bug fix maintenance release should stay with the Cisco IOS Software Release 12.2(18)EW maintenance releases.

Cisco IOS Software Releases 12.1(19)E1 through 12.1(26)E have only the feature set based on Cisco IOS Software Release 12.1(12c)EW1 for the Cisco Catalyst 4500 Series supervisor engines. Customers with Catalyst 4500 Series supervisor engines who require the stability of a maintenance release should migrate from 12.1E releases to the Cisco IOS Software Release 12.2(18)EW maintenance releases.

Contents

This publication consists of these sections:

System Requirements

This section describes the system requirements:

Memory Requirements

These are the minimum required memory configurations for Cisco IOS software on the Catalyst 4500 series switch:

- 256-MB SDRAM DIMM
- 32-MB Flash SIMM

Supported Hardware

The following tables lists the hardware supported on the Catalyst 4500 series switch.

Product Number (append with "=" for spares)	**Product Description**	**Software Version**
		Minimum
Supervisor Engines		
WS-X4013+=	Catalyst 4500 Supervisor Engine II-Plus	12.1(19)EW
WS-X4014=	Catalyst 4000 Supervisor Engine III	12.1(8a)EW
WS-X4015=	Catalyst 4500 Supervisor Engine IV	12.1(12c)EW
WS-X4515/2=	Catalyst 4507R Redundant Supervisor Engine IV	12.1(12c)EW
Gigabit Ethernet Switching Modules		
WS-X4232-GB-RJ	32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	12.1(8a)EW
WS-X4302-GB	2-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	12.1(19)EW
WS-X4306-GB	6-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	12.1(8a)EW
WS-X4418-GB	18-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	12.1(8a)EW
WS-X4412-2GB-T	12-port 1000BASE-T Gigabit Ethernet and 2-GBIC ports switching module	12.1(8a)EW
WS-X4424-GB-RJ45	24-port 10/100/1000BASE-T Gigabit Ethernet switching module	12.1(8a)EW
WS-X4448-GB-LX	48-port 1000BASE-LX Gigabit Ethernet Fiber Optic interface switching module	12.1(8a)EW
WS-X4448-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet switching module	12.1(8a)EW
WS-X4548-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet switching module	12.1(19)EW
Gigabit Interface Converter		
WS-G5483=	1000BASE-T Gigabit Interface Convertor	12.1(13)EW
WS-G5484=	1000BASE-SX Short Wavelength GBIC (multimode only)	12.1(8a)EW
WS-G5486=	1000BASE-LX/LH Long Haul GBIC (single mode or multimode)	12.1(8a)EW
WS-G5487=	1000BASE-ZX Extended Reach GBIC (single-handed)	12.1(8a)EW
DWDM-GBIC-xx.yy	Dense Wavelength-Division Multiplexing Gigabit Interface Convertors	12.1(19)EW
WDM-GBIC-REC	Receive-only 1000BASE-WDM Gigabit Interface Convertors	12.1(19)EW
Fast Ethernet Switching Modules		
WS-X4124-FX-MT	24-port 100BASE-FX Fast Ethernet switching module	12.1(8a)EW
WS-X4148-FX-MT	48-port 100BASE-FX Fast Ethernet switching module	12.1(8a)EW
WS-X4141-FE-LX-MT	48-port 100BASE-LX10 Fast Ethernet switching module	12.1(13)EW
WS-U4504-FX-MT	4-port 100BASE-FX with MTRJ connectors switching module	12.1(8a)EW
Ethernet/Fast Ethernet (10/100) Switching Modules		
WS-X4148-RJ	48-port 10/100-Mbps Fast Ethernet RJ-45 switching module	12.1(8a)EW
WS-X4148-RJ21	48-port 10/100-Mbps Fast Ethernet RJ-21 (telco connector) switching module	12.1(8a)EW

Product Number (append with "=" for spares)	**Product Description**	**Software Version**
		Minimum
WS-X4148-RJ45V	48-port inline power 10/100BASE-TX switching module	12.1(8a)EW for data support 12.1(11b)EW for data and inline power support
WS-X4232-RJ-XX	32-port 10/100 Fast Ethernet RJ-45 modular uplink switching module	12.1(8a)EW
GBIC Modules		
CWDM-GBIC-1470	Longwave 1470 nm laser single-mode	12.1(12c)EW
CWDM-GBIC-1490	Longwave 1490 nm laser single-mode	12.1(12c)EW
CWDM-GBIC-1510	Longwave 1510 nm laser single-mode	12.1(12c)EW
CWDM-GBIC-1530	Longwave 1530 nm laser single-mode	12.1(12c)EW
CWDM-GBIC-1550	Longwave 1550 nm laser single-mode	12.1(12c)EW
CWDM-GBIC-1570	Longwave 1570 nm laser single-mode	12.1(12c)EW
CWDM-GBIC-1590	Longwave 1590 nm laser single-mode	12.1(12c)EW
CWDM-GBIC-1610	Longwave 1610 nm laser single-mode	12.1(12c)EW
Other Modules		
MEM-C4K-FLD64M	Catalyst 4500 CompactFlash, 64 MB Option	12.1(19)EW
MEM-C4K-FLD128M	Catalyst 4500 CompactFlash, 128 MB Option	12.1(19)EW
WS-F4531	Catalyst 4500 Series NetFlow Services Card	12.1(13)EW
PWR-C45-1000AC	Catalyst 4500 1000 Watt AC Power Supply • Data only	12.1(12c)EW
PWR-C45-1400DC	Catalyst 4500 1400 Watt DC Power Supply • with pass through for voice	12.1(13)EW
PWR-C45-1300ACV	Catalyst 4500 1300 Watt AC Power Supply • With integrated voice	12.1(12c)EW
PWR-C45-2800ACV	Catalyst 4500 2800 Watt AC Power Supply • With integrated voice	12.1(12c)EW
WS-P4502-1PSU	Catalyst 4500 Auxiliary Power Shelf (25-slot), including one PWR-4502	12.1(19)EW
PWR-4502	Catalyst 4500 Auxiliary Power Shelf Redundant Power Supply	12.1(19)EW
WS-X4604-GWY	Cisco Catalyst 4500 Access Gateway Module	12.1(13)EW
WS-X4095-PEM	Catalyst 4006 Power Entry module	12.1(11b)EW
WS-P4603-2PSU	Catalyst 4006 Auxiliary Power Shelf (3-slot) including two WS-X4608 power supplies	12.1(11b)EW
WS-X4008-DC	Catalyst 4006 DC Power Supply	12.1(8a)EW
WS-X4008=	Catalyst 4006 AC Power Supply	12.1(11b)EW

Table 1 briefly describes the seven chassis in the Catalyst 4500 series switches. For the chassis listed in the table, refer to Table 2 on page 8 for software version information.

Table 1 Chassis Description

Product Number (append with "=" for spares)	**Description of Modular Chassis**
WS-C4503	Catalyst 4503 chassis includes: • 3 slots • Fan tray • Supports Supervisor Engine IV, Supervisor Engine III, and Supervisor Engine II-Plus, Supervisor Engine II
WS-C4506	Catalyst 4500 chassis includes: • 6 slots • Fan tray • Supports Supervisor Engine IV, Supervisor Engine III, and Supervisor Engine II-Plus, and Supervisor Engine II
WS-C4507R	Catalyst 4500 chassis includes: • 7 slots • Fan tray • Supports Supervisor Engine IV and Supervisor Engine II-Plus
WS-C4006-S4	Catalyst 4006 chassis includes: • 6 slots • Fan tray • 2 AC power supplies • Supports Supervisor Engine IV
WS-C4006-S4-DC	Catalyst 4006 chassis includes: • 6 slots • Fan tray • 2 DC power supplies • Supports Supervisor Engine IV

Table 1 Chassis Description

Product Number (append with "=" for spares)	**Description of Modular Chassis**
WS-C4006-S3-DC	Catalyst 4006 chassis includes: • 6 slots • Fan tray • 2 DC power supplies • Supports Supervisor Engine III
WS-C4006-S3	Catalyst 4006 chassis includes: • 6 slots • Fan tray • 2 AC power supplies • Supports Supervisor Engine III

Table 2 lists the software version information for the Catalyst 4500 supervisor engines.

Table 2 Supervisor Engine Support

Supervisor Engine	**Software Version**
	Minimum
Supervisor Engine II	Catalyst operating system software
Supervisor Engine II-Plus	12.1(19)EW
Supervisor Engine III	12.1(8a)EW
Supervisor Engine IV	12.1(12c)EW

Supported Features

Table 3 lists the Cisco IOS software features for the Catalyst 4500 series switch.

Table 3 Cisco IOS Feature Set for the Catalyst 4500 Series Switch

Layer 1 Features
10/100/1000BASE-TX half duplex and full duplex
1000BASE-SX,-LX, and long haul (-LX/LH, -ZX) full duplex
Longwave laser single mode GBICs[1]
Coarse Wavelength Division Multiplexing (CWDM) GBICs
Dense Wavelength Division Multiplexing (DWDM) GBICs
Layer 2 Bridging Features
Storm control
IP Source Guard
PVRST+

Table 3 Cisco IOS Feature Set for the Catalyst 4500 Series Switch (continued)

Layer 2 transparent bridging[2]
Layer 2 MAC[3] learning, aging, and switching by software
Unicast MAC address filtering
VMPS[4] Client
Layer 2 hardware forwarding at 48 Mpps
Layer 2 switch ports and VLAN trunks
Spanning-Tree Protocol (IEEE 802.1D) per VLAN
802.1s and 802.1w
Layer 2 traceroute
Unidirectional Ethernet port
Per-VLAN spanning tree (PVST) and PVST+
Spanning-tree root guard
Spanning-tree Loop guard and PortFast BPDU Filtering
Support for 9216 byte frames
Port security on PVLANs
Private VLANs
Private VLAN DHCP snooping
ISL[5]-based VLAN encapsulation (excluding blocking ports on WS-X4418-GB and WS-X4412-2GB-T)[6]
IEEE 802.1Q-based VLAN encapsulation
Multiple VLAN access port
VLAN Trunking Protocol (VTP) and VTP domains
Support for 4096 VLANs per switch
Unidirectional link detection (UDLD) and aggressive UDLD
Layer 3 Routing, Switching, and Forwarding
Pragmatic General Multicast
IP and IP multicast routing and switching between Ethernet ports
Static IP routing
PBR[7]
Dynamic Buffer Limiting
QoS-based forwarding based on IP precedence
Trusted boundary
Auto QoS
CEF[8] load balancing
Hardware-based IP CEF routing at 48 Mpps
Up to 128,000 IP routes
Up to 32,000 IP host entries (Layer 3 adjacencies)
Up to 16,000 IP multicast route entries

Table 3 Cisco IOS Feature Set for the Catalyst 4500 Series Switch (continued)

Multicast flooding suppression for STP changes
Software routing of IPX and AppleTalk
IGMPv1, IGMPv2, and IGMPv3 (Full Support)
VRF-lite
Supported Protocols
IS-IS[9]
DTP[10]
RIP[11] and RIP II
IGRP[12]
EIGRP[13]
OSPF[14]
BGP4[15]
MBGP[16]
MSDP[17]
ICMP[18] Router Discovery Protocol
PIM[19]—sparse and dense mode
Static routes
Classless interdomain routing (CIDR)
DVMRP[20]
SSM
EtherChannel Features
Cisco EtherChannel, Fast EtherChannel, and Gigabit EtherChannel technology across line cards
Load balancing for routed traffic, based on source and destination IP addresses
Load sharing for bridged traffic based on MAC addresses
ISL on the Fast EtherChannel and Gigabit EtherChannel
IEEE 802.1Q on the Fast EtherChannel and Gigabit EtherChannel
Bundling of up to eight Fast Ethernet ports
Bundling of up to eight Gigabit Ethernet ports
Up to 64 active Fast Ethernet port channels
Up to 64 active Gigabit Ethernet port channels
Additional Protocols and Features
SPAN CPU port mirroring
SPAN packet-type filtering
SPAN destination in-packets option
RSPAN[21]
Enhanced VLAN statistics
Netflow version 8
NetFlow Statistics Collection

Table 3 Cisco IOS Feature Set for the Catalyst 4500 Series Switch (continued)

NetFlow Statistics Export Version 1 and Version 5
Secondary addressing
Bootstrap protocol (BOOTP)
Authentication, authorization, and accounting using TACACS+ and RADIUS protocol
Cisco Discovery Protocol (CDP)
Cisco Group Management Protocol (CGMP) server support
HSRP[22] over 10/100 Ethernet, Gigabit Ethernet, Fast EtherChannel, and Gigabit EtherChannel
IGMP[23] snooping version1, version 2, and version 3 (Full Support)
IGMP filtering
Port Aggregation Protocol (PagP)
802.3ad LACP
SSH version 1 and version 2[24]
Inline power preallocation
show interface capabilities command
IfIndex persistence
UDLR[25]
Enhanced SNMP MIB support
SNMP[26] version 1, version 2, and version 3
SNMP version 3 (with encryption)
DHCP server and relay-agent
DHCP snooping
802.1x port-based authentication
Port flood blocking
Router standard and extended ACLs [27]on all ports with no performance penalty
Extended IPX Access Control Lists
VLAN Access Control Lists
PACL[28]
Local Proxy ARP
Dynamic ARP Inspection on PVLANs
Dynamic ARP Inspection
Per-port QoS[29] rate-limiting and shaping
Inline power support for Cisco IP phones
Power redundancy
RPR[30]
IPX performance enhancements

1. GBICs = 1470, 1490, 1510, 1530, 1550, 1570, 1590, and 1610 nm
2. This is hardware-based transparent bridging within a VLAN.
3. MAC = Media Access Control

4. VMPS = VLAN Management Policy Server
5. ISL = Inter-Switch Link
6. Ports 3 thru 18 on the WS-X4418-GB and ports 1 thru 12 on the WS-X4412-2GB
7. PBR = policy-based routing
8. CEF = Cisco Express Forwarding
9. IS-IS = Intermediate System to Intermediate System
10. DTP = Dynamic Trunking Protocol
11. RIP = Routing Information Protocol
12. IGRP = Interior Gateway Routing Protocol
13. EIGRP = Enhanced Interior Gateway Routing Protocol
14. OSPF = Open Shortest Path First
15. BGP4 = Border Gateway Protocol 4
16. MBGP = Multicast Border Gateway Protocol
17. MSDP = Multicast Source Discovery Protocol
18. ICMP = Internet Control Message Protocol
19. PIM = Protocol Independent Multicast
20. DVMRP = Distance Vector Multicast Routing Protocol
21. RSPAN = Remote SPAN
22. HSRP = Hot Standby Router Protocol
23. IGMP = Internet Group Management Protocol
24. SSH = Secure Shell Protocol
25. UDLR = Unidirectional Link Detection
26. SNMP = Simple Network Management Protocol
27. ACLs = Access Control Lists
28. PACL = Port Access Control List
29. QoS = Quality of Service
30. RPR = Supervisor redundancy

Unsupported Features

These features are not supported in Cisco IOS Release 12.1(EW2 for the Catalyst 4500 series switch:

- Bridge groups
- Cisco IOS software-based transparent bridging (also called “fallback bridging”)
- Kerberos support for access control
- Community VLANs and two-way community VLANs in private VLANs
- DLSw (data-link switching)
- CLNS routing
- WCCP (Web Cache Communication Protocol)
- Cisco IOS IPX ACLs:
  - <1200-1299> IPX summary address access list
- The following ACL types:
  - Standard Xerox Network System (XNS) access list
  - Extended XNS access list
  - DECnet access list

– Protocol type-code access list

New and Changed Information

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

New Hardware Features in Release 12.1(20)EW2

There are no new hardware features in Release 12.1(20)EW2.

New Software Features in Release 12.1(20)EW2

There are no new software features in Release 12.1(20)EW2.

New Hardware Features in Release 12.1(20)EW1

There are no new hardware features in Release 12.1(20)EW1.

New Software Features in Release 12.1(20)EW1

There are no new software features in Release 12.1(20)EW1.

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

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)
- 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.

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

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 following 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)

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 software 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 version of Cisco IOS software does not require a ROMMON upgrade. However, if you are running an early release of Cisco IOS software and plan to upgrade, the following table lists the recommended ROMMON version.

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

Supervisor Engine	Minimum Cisco IOS Release
III	12.1(8a)EW or 12.1(14)E
IV	12.1(12c)EW or 12.1(14)E
II-Plus	12.1(19)EW

Supervisor Engine	Minimum ROMMON Version
III	12.1(11br)EW
IV	12.1(12r)EW
II-Plus	12.1(19r)EW

ROMMON Version	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

The following sections describe how to upgrade your switch software:

- Upgrading the Supervisor Engine ROMMON from the Console, page 21
- Upgrading the Supervisor Engine ROMMON Remotely Using Telnet, page 24
- Upgrading the Cisco IOS Software, page 28

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 software Release 12.1(20)EW2. For other versions, replace the ROMMON version and Cisco IOS software release with the appropriate versions 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 will be 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 issue 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 a 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 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 0x2102

Switch#
```

The ROMMON has now been upgraded.

See the "Upgrading the Supervisor Engine ROMMON Remotely Using Telnet" section on page 24 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Supervisor Engine ROMMON Remotely Using Telnet

Note You cannot upgrade to version 12.1(19)EW ROMMON with Telnet access.

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 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 issue 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)EW2.

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 will be disconnected during the ROMMON upgrade, so you will not see this output. This step could take 2-3 minutes to complete. You will need to reconnect your Telnet session after 2-3 minutes when the Cisco IOS software image and the interfaces are loaded.

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

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 Supervisor Engine ROMMON Remotely Using Telnet" section on page 24 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Cisco IOS Software

If you have Cisco IOS software Release 12.1(8a)EW loaded on your switch, you must upgrade the ROMMON before upgrading your switch software. For more information, see the "Upgrading the Supervisor Engine ROMMON from the Console" section on page 21.

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

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

Step 1 Download Cisco IOS software 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 will be upgraded.

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

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 software 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:

- 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
- For NFL, the following are not supported:

  - The following packets are not accounted for by the NetFlow Services card:

    Control packets

    Packets with link-level errors

    ARP, RARP
  - Software flow cache size is fixed.
  - Distribution is not based on IP packet size.
- For PBR, the following are not supported:
  - Matching cannot be performed on packet lengths.
  - IP precedence, TOS, and QoS group are fixed.
  - ACL or route-map statistics cannot be updated.
- Supervisor Engine II-Plus cannot read a CompactFlash card formatted by Supervisor Engine III or 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 can occur if a backup configuration file was used.
- A Layer 2 LACP channel cannot be configured with the spanning tree Portfast feature.
- Netbooting using a boot loader image is not supported. See the "Troubleshooting" section on page 73 for details on alternatives.
- There is no support for downgrading to 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 bug CSCdz59058.
- Be aware of the following standard Cisco IOS software behavior when deploying 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 GE 1/1, 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 GE1/1 is no longer present. This is the correct behavior. When the formerly active supervisor engine is reinserted in slot 1, there is no configuration for interface Gig 1/1.

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

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

  ```
  Sup4#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 sample output of the **show standby GigabitEthernet1/1** command:

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

- To have HSRP "preempt delay" 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.

  You will need the **standby delay reload** option in case the router is coming up after a reload.

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

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

- Catalyst 4000 WS-X4124-FX-MT modules with hardware revisions 1.5 and earlier only are supported with the Supervisor Engines I (WS-X4012) and II (WS-X4013).

  Workaround: Contact your technical support representative for a replacement.

- You can run .1q-in-.1q packet pass-through with the Supervisor Engine III and IV, but you cannot run .1q-in-.1q encapsulation with any Catalyst 4000 supervisor engine.
- For PVST and 4K VLANs, Cisco IOS software Releases 12.1(13)EW (and higher) supports a maximum of 3000 spanning tree port instances. If you want to use more than this number of instances, you should use MST rather than PVST.
- Only ports 1 and 2 on the WS-X4418-GB and only ports 13 and 14 on the WS-X4412-2GB-T module can be set as ISL trunks.
- The Fast Ethernet port (10/100) on the supervisor module is active only in ROMMON mode.
- If an original packet is dropped due to transmit queue shaping and/or sharing configurations, a SPAN packet copy can still be transmitted on the SPAN port.
- Do not use over 100,000 routes with Cisco IOS software 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.
- Use the **no ip unreachables** command on all interfaces with ACLs configured for performance reasons.
- Cisco IOS software 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 support a maximum of 16,000 IGMP snooping group entries.
- Layer 3 path load balancing metrics are not supported in Cisco IOS software 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 CLI contains some commands that are not supported in Cisco IOS software Releases 12.1(8a)EW, 12.1(11b)EW, 12.1(12c)EW, 12.1(13)EW, and 12.1(20)EW. (CSCdw44274)
- The threshold for the Dynamic Arp Inspection err-disable function is set to 15 ARP packets per second per interface. You should fine tune 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 Supervisor Engine II-Plus. To take full advantage of the IP source guard feature, you should use the Catalyst 4500 Supervisor Engine IV.

Caveats

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

Open Caveats in Software Release 12.1(20)EW3

This section lists the open caveats in Cisco IOS software Release 12.1(20)EW3.

- For Cisco IOS software 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 Software Release 12.1(20)EW3

This section lists 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 Software Release 12.1(20)EW2

This section lists the open caveats in Cisco IOS software Release 12.1(20)EW2.

- For Cisco IOS software 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 Software Release 12.1(20)EW2

This section lists resolved caveats in Release 12.1(20)EW2:

- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability. (CSCed27956, CSCed38527, CSCed93836, and CSCdz84583)

  This advisory is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-ios, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-nonios

- Symptoms: A router may reload unexpectedly after it attempts to access a low memory address.

  Conditions: This symptom is observed after ACLs have been updated dynamically or after the router has responded dynamically to an IDS signature.

  Workaround: Disable IP Inspect and IDS. (CSCed35253)

- Cisco Internetwork Operating System (IOS) Software releases trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS). (CSCed68575)

This advisory is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-snmp

Open Caveats in Software Release 12.1(20)EW1

This section lists the open caveats in Cisco IOS software Release 12.1(20)EW1.

- For Cisco IOS software 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)

Open Caveats in Software Release 12.1(20)EW

This section lists the open caveats in Release 12.1(20)EW.

- For Cisco IOS software 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 linecard), 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 Software 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 Software 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 Software 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
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 Software 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 Software 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 linecard 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 linecard before bootup and reconnect them after the linecard is online.

  – Disable the link partner for all connected ports on the linecard before bootup and reenable the link partner after the linecard 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 Software 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 linecard 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 linecard before bootup and reconnect them after the linecard is online.
  - Disable the link partner for all connected ports on the linecard before bootup and reenable the link partner after the linecard 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 Software Release 12.1(19)EW

This section lists the resolved caveats in Release 12.1(19)EW:

- 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 Release 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 Software 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 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 Release 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 Software 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 Software 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 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 Release 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 Software 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)

- 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 images for the Releases 12.1(12c)EW2, 12.1(13)EW2, 12.1(19)EW, and 12.1(20)E.

  Workaround: None. (CSCeb59442)

Open Caveats in Software 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)

- 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 images for Releases 12.1(12c)EW2, 12.1(13)EW2, 12.1(19)EW, and 12.1(20)E.

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 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 Release 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 Software 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 4500 series switch running Release 12.1(13)EW, the switch reloads unexpectedly; this command is not supported in Release 12.1(13)EW.

  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 Software 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)

- 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 images for Releases 12.1(12c)EW2, 12.1(13)EW2, 12.1(19)EW, and 12.1(20)E.

  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 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 Release 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 Software 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 may take over from the active supervisor 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 result in unexpected behavior.

  Workaround: Don't configure 802.1x on PVLAN ports. (CSCdy23098)

Open Caveats in Software 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 may take over from the active supervisor 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 Software 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 Software 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 may take over from the active supervisor 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 Software 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)

- 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 images for Releases 12.1(12c)EW2, 12.1(13)EW2, 12.1(19)EW, and 12.1(20)E.

  Workaround: None. (CSCeb59442)

Open Caveats in Software 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)

- 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 images for Releases 12.1(12c)EW2, 12.1(13)EW2, 12.1(19)EW, and 12.1(20)E.

  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 may take over from the active supervisor 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 Software 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 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 running Release 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 software Release 12.1(12c)EW.

  Workaround: Avoid configuring ACLs that trigger L4 operator expansion. (CSCdy70646)

Open Caveats in Software 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 images for Releases 12.1(12c)EW2, 12.1(13)EW2, 12.1(19)EW, and 12.1(20)E.

  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 may take over from the active supervisor 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 Software 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 Software 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 Software 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 Software 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 Software 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 software 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 software Release 12.1(8a)EW. (CSCdw59733)

Open Caveats in Software 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 software 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 software Release 12.1(8a)EW. (CSCdw59733)

Resolved Caveats in Software 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 Software 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 software 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 software Release 12.1(8a)EW. (CSCdw59733)

Resolved Caveats in Software Release 12.1(8a)EW

There are no resolved caveats in software Release 12.1(8a)EW.

Troubleshooting

These sections provide troubleshooting guidelines for the Catalyst 4000 family running IOS supervisor engines:

Netbooting from the ROMMON

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

1. Boot from a CompactFlash card by entering the following command:

   ```
   rommon 1> boot slot0:<bootable_image>
   ```

2. Use ROMMON TFTP boot.

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

   - the BOOTLDR variable should *not* be set
   - the TFTP server must be accessible from the 10/100 port on the supervisor engine.

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

a. Ensure that the 10/100 port on the supervisor engine is physically connected to the network.

b. Verify that bootloader environment is not set by entering the **unset bootldr** command.

c. Set IP address of the 10/100 port on the supervisor engine by entering the following command: **set interface fa1** *ip_address*> <*ip_mask*

   For example, to set the supervisor Ethernet port with an IP address 172.16.1.5 and IP mask 255.255.255.0.0, enter the following command:

   ```
   rommon 2> set interface fa1 172.16.1.5 255.255.0.0
   ```

d. Set default gateway for the 10/100 port on the supervisor engine by entering the following command: **set ip route default** *gateway_ip_address*. The default gateway should be directly connected to the supervisor engine 10/100 port subnet.

e. Ping the TFTP server to ensure that there is connectivity to the server from the 10/100 port on the supervisor engine by entering the following command: **ping** <*tftp_server_ip_address*>.

f. Once the ping is successful, boot the image from the TFTP server by entering the following command: **boot tftp://***tftp_server_ip_address*>**/**<*image_path_and_file_name*

   For example, to boot the image name cat4000-is-mz.160 located on the TFTP server 172.16.1.8, enter the following command:

   ```
   rommon 3> boot tftp://172.16.1.8/tftpboot/cat4000-is-mz
   ```

Troubleshooting at the System Level

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.
- Ensure that you do not mix the serial and ethernet cables plugged into the supervisor engine. The Fast Ethernet port (10/100 MGT) on the supervisor engine is inoperative in Cisco IOS Releases 12.1(8a)EW, 12.1(11b)EW, 12.1(12c)EW, 12.1(13)EW, and 12.1(19)EW. An Ethernet cable plugged into the Fast Ethernet port is active only in ROMMON mode.

Troubleshooting Modules

This section contains troubleshooting guidelines for modules:

- When you hot insert a module into a chassis, always use the ejector levers on the front of the module to seat the backplane pins properly. Inserting a module without using the ejector levers might cause the supervisor engine to display incorrect messages about the module. For module installation instructions, refer to the *Catalyst 4500 Series Module Installation Guide*.
- Whenever you connect an interface that has duplex set to autonegotiate to an end station or another networking device, ensure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the port set to autonegotiate will remain in half-duplex mode, which can cause a duplex mismatch resulting in packet loss, late collisions, and line errors on the link.

Troubleshooting VLANs

Although DTP is a point-to-point protocol, some internetworking devices might forward DTP frames. To avoid connectivity problems that might be caused by a switch acting on these forwarded DTP frames, do the following:

- For interfaces connected to devices that do not support DTP, in which trunking is not currently being used, configure interfaces with the **switchport mode access** command, which puts the interface into access mode and causes it to stop sending DTP frames.
- When manually enabling trunking on a link to devices that do not support DTP, use the **switchport nonegotiate** and **switchport mode trunk** commands, which puts the interface into trunking mode without sending DTP frames.

Troubleshooting Spanning Tree

The Spanning Tree Protocol (STP) blocks certain ports to prevent physical loops in a redundant topology. On a blocked port, switches periodically receive spanning tree bridge protocol data units (BPDUs) from neighboring switches. You can configure the frequency with which BPDUs are received by entering the **spanning-tree VLAN** *vlan_ID* **hello-time** command. By default, the frequency is set to 2 seconds. If a switch does not receive a BPDU in the time period defined by the **spanning-tree VLAN** *vlan_ID* **max-age** command (20 seconds by default), the blocked port transitions to the listening state, the learning state, and to the forwarding state. As it transitions, the switch waits for the time period specified by the **spanning-tree VLAN** *vlan_ID* **forward-time** command (15 seconds by default) in each of these intermediate states. Therefore, a blocked spanning tree interface moves into the forwarding state if it does not receive BPDUs from its neighbor within approximately 50 seconds.

Note We do not recommend using the UplinkFast feature on switches with more than 20 active VLANs because convergence times might be unacceptably long.

Use these guidelines to debug STP problems:

- Ensure that the sum of the logical interfaces across all instances of spanning tree for different VLANs does not exceed 3000 for the Supervisor Engine IV and 1500 for Supervisor Engine II-Plus. The sum of all logical interfaces equals the number of trunks on the switch multiplied by the number of active VLANs on the trunks, plus the number of non-trunking interfaces on the switch. Note the following:
  - When numerous protocol features (such as VTP pruning, EtherChannel, and RMON) are enabled concurrently, the number of supported logical spanning tree interfaces is reduced. To maintain the number of supported logical spanning tree interfaces, keep switched traffic off the management VLAN.

  The **show spanning-tree summary totals** command displays the number of logical interfaces in the **STP Active** column.
- For networks with large numbers of spanning tree instances, use 802.1s Multiple Spanning Tree (MST) mode. Refer to the "Understanding and Configuring Multiple Spanning Tree" chapter in the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.
- Keep track of all blocked spanning tree interfaces in each switch in your network. For each of the blocked spanning tree ports, keep track of the output of the **show interface** command. Check to see if the interface has registered a lot of alignment, FCS, or any other type of line errors. If these errors

are incrementing continuously, the interface might drop input BPDUs. If the **input queue** counter is incrementing continuously, the interface is losing input packets because of a lack of receive buffers. This problem can also cause the interface to drop incoming BPDUs.

- On a blocked spanning tree interface, check the duplex configuration to ensure that the interface duplex is set to the same mode as the interface of its neighboring device.
- On trunks, ensure that the trunk configuration is set properly on both sides of the link.
- On trunks, if the neighboring device supports it, set duplex to full on both sides of the link to prevent any collisions during times of heavy traffic.

Troubleshooting MIBs

For general information on MIBs, RMON groups, and traps, refer to the Cisco public MIB directory (http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml). For information on the specific MIBs supported by the Catalyst 4500 series switches, refer to the Catalyst 4000 MIB Support List located at ftp://ftp.cisco.com/pub/mibs/supportlists/cat4000/cat4000-supportlist.html.

Documentation Updates for Release 12.1(20)EW2

None.

Related Documentation

Although their Release Notes are unique, the 4 platforms (Catalyst 4500, Catalyst 4900, Catalyst ME 4900, and Catalyst 4900M) use the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide*. Refer to the following home pages for additional information:

- Catalyst 4500 Series Switch Documentation Home

  http://www.cisco.com/go/cat4500/docs
- Catalyst 4900 Series Switch Documentation Home

  http://www.cisco.com/go/cat4900/docs
- Cisco ME 4900 Series Ethernet Switches Documentation Home

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

Hardware Documents

Installation guides and notes including specifications and relevant safety information are available at the following URLs:

- *Catalyst 4500 Series Switches Installation Guide*

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/installation/guide/78-14409-08/4500inst.html
- *Catalyst 4500 E-series Switches Installation Guide*

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/catalyst4500e/installation/guide/Eseries.html

- For information about individual switching modules and supervisors, refer to the *Catalyst 4500 Series Module Installation Guide* at:

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

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

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

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

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

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

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

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

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

Software Documentation

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

- Catalyst 4500 release notes are available at:

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

- Catalyst 4900 release notes are available at:

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

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

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

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

- *Catalyst 4500 Series Software Configuration Guide*

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

- *Catalyst 4500 Series Software Command Reference*

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

- *Catalyst 4500 Series Software System Message Guide*

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

Cisco IOS Documentation

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

- Cisco IOS configuration guides, Release 12.x

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

- Cisco IOS command references, Release 12.x

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

  You can also use the Command Lookup Tool at:

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

- Cisco IOS system messages, version 12.x

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

  You can also use the Error Message Decoder tool at:

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

- For information about MIBs, refer to:

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

Obtaining Documentation and Submitting a Service Request

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

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

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

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

Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Release 12.1(20)EW2