Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Release 12.1(19)E

Current Release
12.1(19)E—May 27, 2003

Previous Releases
12.1(14)E1, 12.1(12c)EW1, 12.1(12c)EW, 12.1(11b)EW1, 12.1(11b)EW, 12.1(8a)EW1, 12.1(8a)EW

Product Numbers:

- S4KL3-12119E—Cisco IOS for the Catalyst 4000 Family Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(19)E
- S4KL3E-12119E—Cisco IOS for the Catalyst 4000 Family Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(19)E
- S4KL3-12114E—Cisco IOS for the Catalyst 4000 Family Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(14)E1
- S4KL3E-12114E—Cisco IOS for the Catalyst 4000 Family Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(14)E1
- S4KL3-12112EW—Cisco IOS for the Catalyst 4000 Family Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(12c)EW
- S4KL3E-12112EW—Cisco IOS for the Catalyst 4000 Family Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(12c)EW
- S4KL3-12111EW—Cisco IOS for the Catalyst 4000, basic Layer 3 software image (RIP, Static Routes), Release 12.1(11b)EW
- S4KL3E-12111EW—Cisco IOS for the Catalyst 4000, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(11b)EW1
- S4KL3-12108EW—Cisco IOS for the Catalyst 4000, basic Layer 3 software image (RIP, Static Routes), Release 12.1(8a)EW
- S4KL3E-12108EW—Cisco IOS for the Catalyst 4000, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(8a)EW1

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

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 version 12.1(19)E.

Note The 12.1(19)E release contains only the software and hardware functionality up to and including Catalyst 4500 IOS release 12.1(12c)EW1. Subsequent releases on the 12.1E train will be maintenance releases with the Catalyst 4500 12.1(12c)EW1 feature set. The 12.1E train is on the General Deployment (GD) track. The 12.1E IOS releases are for Catalyst 4500 customers who require the stability of a GD release with a fixed set of features.
As of May 2003, 12.1(13)EW is the latest 12.1EW IOS release for the Catalyst 4500. Software features such as PBR, DBL, Port Security, Jumbo Frames, as well as support for the Catalyst 4500 NetFlow Services Card, 1000BASE-T GBIC and the AGM module are contained in this release. The Catalyst 4500 12.1EW IOS release train will continue to be the vehicle to offer the latest hardware and software features.

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 on the Catalyst 4500 series switch:

- 256-MB SDRAM DIMM

- 64-MB Flash SIMM

Supported Hardware

Product Number (append with "=" for spares)	**Product Description**	**Software Version**
		Minimum
Supervisor Engines		
WS-X4014=	Cisco Catalyst 4500 Supervisor Engine III	12.1(8a)EW
WS-X4515=	Cisco Catalyst 4500 Supervisor Engine IV	12.1(12c)EW
WS-X4515/2=	Cisco 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-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
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-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
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

Product Number (append with "=" for spares)	**Product Description**	**Software Version**
		Minimum
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		
WS-X4095-PEM	Catalyst 4000 Power Entry module	12.1(11b)EW
WS-P4603-2PSU	Catalyst 4000 Auxiliary Power Shelf (3-slot) including two WS-X4608 power supplies	12.1(11b)EW
WS-X4008-DC	Catalyst 4000 DC Power Supply	12.1(8a)EW
WS-X4008=	Catalyst 4000 AC Power Supply	12.1(11b)EW
PWR-C45-1000AC	Catalyst 4500 1000 Watt AC Power Supply • Data only	12.1(12c)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
Modular Chassis		
WS-C4006	Cisco 4006 chassis: • 1024 MAC addresses • 6 slots • Fan • Redundant supervisor incapable • Supports Supervisor Engine IV, Supervisor Engine III, and Supervisor Engine II	12.1(8a)EW
WS-C4503	Cisco 4503 chassis: • 64 MAC addresses • 3 slots • Fan • Power supply not provided with chassis • Redundant supervisor incapable • Supports Supervisor Engine IV, Supervisor Engine III, and Supervisor Engine II	12.1(12c)EW

Product Number (append with "=" for spares)	**Product Description**	**Software Version**
		Minimum
WS-C4506	Cisco Catalyst 4500 chassis: • 64 MAC addresses • 6 slots • Fan • Power supply not provided with chassis • Redundant supervisor incapable • Supports Supervisor Engine IV, Supervisor Engine III, and Supervisor Engine II	12.1(12c)EW
WS-C4507R	Cisco Catalyst 4500 chassis: • 64 MAC addresses • 7 slots • Fan • Power supply not provided with chassis • Redundant supervisor capable • Supports Supervisor Engine IV only	12.1(12c)EW

Supported Features

Table 1 lists the software features for the Catalyst 4500 series switch.

Table 1 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]
Layer 2 Bridging Features
Layer 2 transparent bridging[2]
Layer 2 MAC[3] learning, aging, and switching by software
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
Per-VLAN spanning tree (PVST) and PVST+
Spanning-tree root guard
Spanning-tree Loop guard and PortFast BPDU Filtering
Support for 1600 byte frames

Table 1 Feature Set for the Catalyst 4500 Series Switch (continued)

Private VLANs
ISL[4]-based VLAN encapsulation (excluding blocking ports on WS-X4418-GB and WS-X4412-2GB-T)[5]
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
IP and IP multicast routing and switching between Ethernet ports
Static IP routing
QoS-based forwarding based on IP precedence
CEF[6] load balancing
Hardware-based IP CEF routing at 48Mpps
Up to 128,000 IP routes
Up to 32,000 IP host entries (Layer 3 adjacencies)
Up to 12,000 IP multicast route entries
Multicast flooding suppression for STP changes
Software routing of IPX and AppleTalk
IGMP v1, v2, and v3
Supported Protocols
DTP[7]
RIP[8] and RIP II
IGRP[9]
EIGRP[10]
OSPF[11]
BGP4[12]
MBGP[13]
MSDP[14]
ICMP[15] Router Discovery Protocol
PIM[16]—sparse and dense mode
Static routes
Classless interdomain routing (CIDR)
DVMRP[17]
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

Table 1 Feature Set for the Catalyst 4500 Series Switch (continued)

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
Secondary addressing
Bootstrap protocol (BOOTP)
Authentication using TACACS+ and RADIUS protocol
Cisco Discovery Protocol (CDP)
Cisco Group Management Protocol (CGMP) server support
HSRP[18] over 10/100 Ethernet, Gigabit Ethernet, Fast EtherChannel, and Gigabit EtherChannel
IGMP[19] snooping v1 and v2
IGMP filtering
Port Aggregation Protocol (PagP)
SNMP[20] v1 and v2
DHCP server and relay-agent
DHCP snooping
802.1x port-based authentication
Router standard and extended ACLs [21]on all ports with no performance penalty
VLAN Access Control Lists
Local Proxy ARP
Per-port QoS[22] rate-limiting and shaping
Inline power support for Cisco IP phones
Power redundancy
RPR[23]

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. ISL = Inter-Switch Link
5. Ports 3 thru 18 on the WS-X4418-GB and ports 1 thru 12 on the WS-X4412-2GB
6. CEF = Cisco Express Forwarding
7. DTP = Dynamic Trunking Protocol
8. RIP = Routing Information Protocol
9. IGRP = Interior Gateway Routing Protocol
10. EIGRP = Enhanced Interior Gateway Routing Protocol
11. OSPF = Open Shortest Path First
12. BGP4 = Border Gateway Protocol 4
13. MBGP = Multicast Border Gateway Protocol
14. MSDP = Multicast Source Discovery Protocol

15. ICMP = Internet Control Message Protocol
16. PIM = Protocol Independent Multicast
17. DVMRP = Distance Vector Multicast Routing Protocol
18. HSRP = Hot Standby Router Protocol
19. IGMP = Internet Group Management Protocol
20. SNMP = Simple Network Management Protocol
21. ACLs = Access Control Lists
22. QoS = Quality of Service
23. RPR = Supervisor redundancy

Unsupported Features

These are some of the features that are not supported in Cisco IOS Release 12.1(19)E for the Catalyst 4500 series switch:

- Bridge groups
- EtherChannel DHCP snooping
  - DHCP snooping on private VLANs
- IOS software-based transparent bridging (also called “fallback bridging”)
- Secure access via secure shell (SSH)
- Access control using authorization and accounting
- Kerberos support for access control
- HTTP server
- Community VLANs and two-way community VLANs in private VLANs
- VLAN Management Policy Server (VMPS) client or server
- Remote SPAN (RSPAN)
- Port security
- WS-X4232-L3
- WS-X4604-GWY
- WS-G5483
- Jumbo frames
- IGMP v3 snooping
- DLSw (Data-link switching)
- WCCP (Web Cache Communication Protocol)
- IEEE 802.3ad
- PBR (policy-based routing)
- 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(19)E

None. This is an E train release.

New Software Features in Release 12.1(19)E

None. This is an E train release.

New Hardware Features in Release 12.1(14)E1

None. This is an E train release.

New Software Features in Release 12.1(14)E1

None. This is an E train release.

New Hardware Features in Release 12.1(12c)EW

Release 12.1(12c)EW provides the following new hardware for the Catalyst 4000 family 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 4000 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 4000 family 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 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 for the Catalyst 4006 switch with Supervisor Engine III. Release 12.1(8a)EW provides these features:

- The Layer 2 features are as follows:
  - 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

If you have a Catalyst 4500 series switch running Cisco IOS 12.1(11b)EW1 or earlier, and you want to upgrade your switch to Cisco IOS 12.1(19)E, you must upgrade the Supervisor Engine III or IV ROMMON version to at least 12.1(12r)EW in addition to upgrading the Cisco IOS software.

The following sections describe how to upgrade your switch software:

- Upgrading the Supervisor Engine ROMMON and the Cisco IOS Software, page 13
- Upgrading the Supervisor Engine ROMMON, page 19
- Upgrading the Cisco IOS Software, page 22

Upgrading the Supervisor Engine ROMMON and the Cisco IOS Software

This section describes how to upgrade the ROMMON software and the Cisco IOS software on your switch in a single procedure. If this process fails, upgrade your ROMMON software as described in "Upgrading the Supervisor Engine ROMMON" section on page 19 and then upgrade your Cisco IOS software as described in "Upgrading the Cisco IOS Software" section on page 22.

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

To upgrade the ROMMON software and Cisco IOS software on your switch follow this procedure:

Step 1 Download the **cat4000-sup3-promupgrade-121_12r_EW** 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-sup3-promupgrade-121_12r_EW** programs are available at the same location on Cisco.com where you download Catalyst 4500 system images.

Step 2 Download the Cisco IOS software version 12.1(19)E image from Cisco.com and place it on a TFTP server in a directory that is accessible from the supervisor to be upgraded.

Step 3 Use the **dir bootflash:** command to ensure that there is sufficient space in Flash to store the **promupgrade** image and the Cisco IOS software 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 Compact Flash card, use **slot0:** instead of **bootflash:**.

Step 4 Download the **cat4000-sup3-promupgrade-121_12r_EW** program into Flash memory using the **copy tftp** command.

The following example shows how to download the **promupgrade** image **cat4000-sup3-promupgrade-121_12r_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 [/home/rommon/4014rommon]? cat4000-sup3-promupgrade-121_12r_EW
Destination filename [cat4000-sup3-promupgrade-121_12r_EW]?
Accessing tftp://172.20.58.78/ cat4000-sup3-promupgrade-121_12r_EW...
Loading cat4000-sup3-promupgrade-121_12r_EW from 172.20.58.78 (via FastEthernet2/1)
:!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 2006316/4012032 bytes]

2006316 bytes copied in 20.936 secs (100315 bytes/sec)
Switch#
```

Step 5 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.121-14.E1** 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-mz.121-14.E1]?
Destination filename [cat4000-is-mz.121-14.E1]?
Accessing tftp://172.20.58.78/cat4000-is-mz.121-14.E1...
Loading cat4000-is-mz.121-14.E1 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 6923388/13846528 bytes]

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

Step 6 Use the **show bootvar** command to display the files specified in the BOOT variable.

The following example shows how to display the contents of the BOOT variable.

```
Switch# show bootvar
```

```
BOOT variable = bootflash:cat4000-is-mz.121-8a.EW
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2100
Switch#
```

Step 7 Enter the **no boot system flash bootflash:***file_name* command to clear the BOOT variable.

The following example shows how to clear the **cat4000-is-mz.121-8a.EW** file and save 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 8 Use the **show bootvar** command to verify that BOOT variable is empty.

The following example shows an empty the BOOT variable.

```
Switch# show bootvar
BOOT variable does not exist
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2100
Switch#
```

Step 9 Use the **boot system flash** command to add the **cat4000-sup3-promupgrade-121_12r_EW** program and the Cisco IOS software image to the BOOT variable.

The following example shows how to add the **cat4000-sup3-promupgrade-121_12r_EW** program and the **cat4000-is-mz.121-14.E1** image to the BOOT variable.

```
Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4000-sup3-promupgrade-121_12r_EW
Switch(config)# boot system flash bootflash:cat4000-is-mz.121-14.E1
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3723 to 1312 bytes [OK]
Switch#
```

Step 10 Use the **show bootvar** command to verify that the BOOT variable contains the promupgrade image and Cisco IOS image, and that the configuration register is set to 0x2102. If the configuration register is not set to 0x2102, proceed to step 11. If the configuration register is set to 0x2102, proceed to step 12.

The following example shows that the **cat4000-sup3-promupgrade-121_12r_EW** program and the **cat4000-is-mz.121-14.E1** image are in the BOOT variable and that the configuration register is set to 0x21020.

```
Switch# show bootvar
BOOT variable = bootflash:cat4000-sup3-promupgrade-121_12r_EW,1;cat4000-is-mz.121-14.E1,1
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
Switch#
```

Step 11 Use the **configure-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)# configure-register 0x2102
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3723 to 1312 bytes [OK]
Switch#
```

Step 12 Enter the **reload** command to reboot and upgrade the switch. The switch upgrades the ROMMON and boots the new Cisco IOS image.

Caution The upgrade and reboot may require up to 15 minutes to complete. Do not disturb your switch during this process. If the process fails during the reboot, you must upgrade the ROMMON (as described in the "Upgrading the Supervisor Engine ROMMON" section on page 19) and then upgrade the Cisco IOS software (as described in "Upgrading the Cisco IOS Software" section on page 22).

The following example shows the output from the upgrade and reboot.

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

00:02:53:%SYS-5-RELOAD:Reload requested

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

    Rom Monitor Program Version 12.1(8r)EW

    Board type 1, Board revision 6
    Swamp FPGA revision 16, Dagobah FPGA revision 43
    ......
    ......
    ***** The system will autoboot in 5 seconds *****

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

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

    config-register = 0x2102
    Autobooting using BOOT variable specified file.....

    Current BOOT file is --- bootflash:cat4000-sup3-promupgrade-121_12r_EW
    ......

**********************************************************
    *                                                    *
    *   Rom Monitor Upgrade Utility For WS-X4014 System     *
    *  This upgrades flash Rom Monitor image to the latest  *
    *                                                    *
    *  Copyright (c) 2002 by Cisco Systems, Inc.            *
    *  All rights reserved.                              *
    *                                                    *
    ******************************************************
```

```
......
Success! The prom 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 6
Swamp FPGA revision 16, Dagobah FPGA revision 48

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

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

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

config-register = 0x2102
Autobooting using BOOT variable specified file.....

Current BOOT file is --- bootflash:cat4000-is-mz.121-14.E1

Rommon reg:0x300041A8

Running diags...

Decompressing the image

##################################################
##################################################
####################

[OK]

k2diags version 1.6

prod:WS-X4014  part:73-6854-06  serial:JAB05450C57

Power-on-self-test for Module 1: WS-X4014
Status:(. = Pass, F = Fail)
....
Module 1 Passed

Exiting to ios...

Rommon reg:0x300001A8

Running IOS...

Decompressing the image
```

```
    ############################################################
    ############################################################
    ############################################################
    ############################################################
    ############################################################
    ############################################################
    ############################################################
    ############################################################
    ############################################################
    ############################################################
    ################################

     [OK]

                   Restricted Rights Legend

     Use, duplication, or disclosure by the Government is
     subject to restrictions as set forth in subparagraph
     (c) of the Commercial Computer Software - Restricted
     Rights clause at FAR sec. 52.227-19 and subparagraph
     (c) (1) (ii) of the Rights in Technical Data and Computer
     Software clause at DFARS sec. 252.227-7013.

               cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

     Cisco Internetwork Operating System Software
     IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-IS-M), Version
     ......
     Uncompressed configuration from 1033 bytes to 3204 bytes

     Press RETURN to get started!
     .....
     Cisco Internetwork Operating System Software
     IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-IS-M), Version
     ......
Switch#
```

Step 13 After the switch has booted, use the **show version** command to confirm the ROMMON and Cisco IOS versions. If the ROMMON or Cisco IOS versions are incorrect, you must upgrade the ROMMON (as described in the "Upgrading the Supervisor Engine ROMMON" section on page 19), and then upgrade the Cisco IOS software (as described in "Upgrading the Cisco IOS Software" section on page 22).

In the following example, the ROMMON level is 12.1(12r)EW, and the Cisco IOS version 12.1(19)E.

```
Switch# show version
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-IS-M), Version
12.1(19)E,  RELEASE SOFTWARE (fc1)
TAC Support:http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Tue 30-Apr-02 17:34 by ccai
Image text-base:0x00000000, data-base:0x00AA2B8C
ROM:12.1(12r)EW
Switch uptime is 6 minutes
System returned to ROM by reload
System image file is "slot0:fcsboot"

cisco WS-C4006 (MPC8245) processor (revision 6) with 262144K bytes of memory.
Processor board ID
Last reset from Reload
48 FastEthernet/IEEE 802.3 interface(s)
```

```
2 Gigabit Ethernet/IEEE 802.3 interface(s)
467K bytes of non-volatile configuration memory.

Configuration register is 0x2102
Switch#
```

Step 14 Use the **delete** command to delete the **promupgrade** program from bootflash: and the **squeeze bootflash:** command to reclaim unused space.

The following example shows how to delete the **cat4000-sup3-promupgrade-121_12r_EW** image from bootflash: and reclaim unused space.

```
Switch# delete bootflash:cat4000-sup3-promupgrade-121_12r_EW
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 15 Use the **no boot system flash** command to delete the **cat4000-sup3-promupgrade-121_12r_EW** image from the BOOT variable.

The following example shows how to delete the **cat4000-sup3-promupgrade-121_12r_EW** image from the BOOT variable.

```
Switch# configure terminal
Switch(config)# no boot system flash cat4000-sup3-promupgrade-121_12r_EW
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3620 to 1236 bytes [OK]
Switch#
```

Step 16 Use the **show bootvar** command to verify that the BOOT variable contains only the Cisco IOS software image.

The following example shows that the BOOT variable contains only the Cisco IOS image **cat4000-is-mz.121-14.E1**.

```
Switch# show bootvar
BOOT variable = bootflash:cat4000-is-mz.121-14.E1,1
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
Switch#
```

Upgrading the Supervisor Engine ROMMON

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

If you have a Catalyst 4500 series switch running Cisco IOS 12.1(11b)EW1 or earlier, and you want to upgrade your switch to Cisco IOS 12.1(19)E, you must upgrade the Supervisor Engine ROMMON version to at least 12.1(12r)EW. When you upgrade and boot the Cisco IOS software to 12.1(19)E, the field programmable gate array (FPGA) is automatically upgraded.

Follow this procedure to upgrade your Supervisor Engine ROMMON to 12.1(12r)EW:

Step 1 Directly connect a serial cable to the console port of the Supervisor Engine III.

> **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-sup3-promupgrade-121_12r_EW** 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-sup3-promupgrade-121_12r_EW** programs are available at the same location on Cisco.com where you download Catalyst 4500 system images.

Step 3 Use the **dir bootflash:** command to ensure that there is sufficient space in Flash 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 Compact Flash card, use **slot0:** instead of **bootflash:**.

Step 4 Download the **cat4000-sup3-promupgrade-121_12r_EW** program into Flash memory using the **copy tftp** command.

The following example shows how to download the **promupgrade** image **cat4000-sup3-promupgrade-121_12r_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-sup3-promupgrade-121_12r_EW]?
Destination filename [cat4000-sup3-promupgrade-121_12r_EW]?
Accessing tftp://172.20.58.78/ cat4000-sup3-promupgrade-121_12r_EW...
Loading cat4000-sup3-promupgrade-121_12r_EW from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 2006316/4012032 bytes]

2006316 bytes copied in 20.936 secs (100315 bytes/sec)
Switch#
```

Step 5 Enter the **reload** command to reset the switch and 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-X4014 System.          *
 * Copyright (c) 2002 by Cisco Systems, Inc.            *
 * All rights reserved.                                 *
 *                                                      *
 ********************************************************

 Rom Monitor Program Version 12.1(8r)EW

.
.(output truncated)
.

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

Step 6 Run the prompupgrade program by entering the **boot bootflash:cat4000-sup3-promupgrade-121_12r_EW** command.

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, OIR of the supervisor, etc., for at least five minutes.

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

```
rommon 2 > boot bootflash:cat4000-sup3-promupgrade-121_12r_EW
Rommon reg:0x300001A8
Decompressing the image
################################################################################################
################################################################################################
################################################################################################
################################################################################################
################################################################################################
################################################################################################
######### [OK]

              Restricted Rights Legend

********************************************************
 *                                                      *
 * Rom Monitor Upgrade Utility For WS-X4014 System      *
 * This upgrades flash Rom Monitor image to the latest  *
 *                                                      *
 * Copyright (c) 2002 by Cisco Systems, Inc.            *
 * All rights reserved.                                 *
 *                                                      *
 ********************************************************

 Image size = 431.476 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  (0x6bddc 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 seconds.
0
```

Step 7 Boot IOS version 12.1(19)E and enter the show version command to verify that ROMMON has been upgraded to 12.1(12r)EW.

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

The following example shows how to delete the **cat4000-sup3-promupgrade-121_12r_EW** image from bootflash and reclaim unused space.

```
Switch# delete bootflash:cat4000-sup3-promupgrade-121_12r_EW
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#
```

The ROMMON is now upgraded.

See the "Upgrading the Cisco IOS Software" section on page 22 for instructions on upgrading the Cisco IOS software on your switch.

Upgrading the Cisco IOS Software

You can upgrade the Cisco IOS software on your Catalyst 4500 series switch using the following procedure.

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" section on page 19.

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

Step 1 Download the Cisco IOS software version 12.1(12r)EW image from Cisco.com and place it on a TFTP server in a directory that is accessible from the supervisor to 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 Compact Flash 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.121-14.E1** 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_14.E1]?
Destination filename [cat4000-is-mz.121-14.E1]?
Accessing tftp://172.20.58.78/cat4000-is-mz.121-14.E1
Loading cat4000-is-mz.121-14.E1 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** command to clear the BOOT variable.

The following example shows how to clear the BOOT variable.

```
Switch# configure terminal
Switch(config)# no boot system flash
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.121-14.E1** image to the BOOT variable.

```
Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4000-is-mz.121-14.E1
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

Step 6 Use the **configure-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)# configure-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, OIR of the supervisor, etc., for at least five minutes!

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

```
Switch# reset
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 version is running on the switch.

Limitations and Restrictions

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

- For IPX software routing, the following are not supported:
  - NHRP (Next Hop Resolution Protocol)
  - NLSP
- For AppleTalk software routing, the following are not supported:
  - AURP
  - AppleTalk Control Protocol for PPP
- 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 and remove the CLI. Here is a sample output of the **[no standby group# name] show standby GigabitEthernet1/1** command:

```
GigabitEthernet1/1 - Group 0
  Local state is Active, priority 105, may preempt
  Hellotime 1 sec, holdtime 3 sec
  Next hello sent in 0.642
  Virtual IP address is 131.241.2.6 configured
    Secondary virtual IP address 131.241.2.7
  Active router is local
  Standby router is 131.241.2.2 expires in 2.872
  Virtual mac address is 0000.0c07.ac00
  2 state changes, last state change 00:00:41
  IP redundancy name is "hsrp-Gi1/1-0" (default) <====== this line should be removed
  Priority tracking 1 interface, 1 up:
```

```
Interface                   Decrement  State
GigabitEthernet1/2             10      Up
```

- 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 don't 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 4500 series WS-X4124-FX-MT modules with hardware revisions 1.5 and lower are only supported with the Supervisor Engines I (WS-X4012) and II (WS-X4013).

  Workaround: Contact your technical support representative for a replacement.

- UDLD does not work on ISL trunks and on ports in a Layer 3 port channel on a Catalyst 4500 series switch with a Supervisor Engine III (WS-X4014). This caveat is present in releases 12.1(8a)EW, 12.1(8a)EW1, 12.1(11b)EW, 12.1(11b)EW1, 12.1(12c)EW, 12.1(12c)EW1, 12.1(14)E1, and 12.1(19)E.
- 1q in 1q packet pass-through procedure is supported with the Supervisor Engine III and IV, but 1q in 1q encapsulation is not supported with any Catalyst 4500 Supervisor Engine.
- For PVST and 4k VLANs, Cisco IOS software release 12.1(19)E 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.
- We recommend that you 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(14)E1, and 12.1(19)E.
- We recommend that you 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, and 12.1(12c)EW support a maximum of 16,000 IGMP snooping group entries.
- BGP Policy accounting is not supported in Cisco IOS software releases 12.1(8a)EW, 12.1(11b)EW, and 12.1(12c)EW. (CSCdv20786)
- BGP Conditional Advertisement are not supported in Cisco IOS software releases 12.1(8a)EW, 12.1(11b)EW, and 12.1(12c)EW. (CSCdv20786)
- Layer 3 path load balancing metrics are not supported in Cisco IOS software releases 12.1(8a)EW, 12.1(11b)EW, and 12.1(12c)EW. (CSCdv10578)
- The CLI contains some commands that are not supported in Cisco IOS software releases 12.1(8a)EW, 12.1(11b)EW, and 12.1(12c)EW. (CSCdw44274)

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(19)E

This section lists open caveats in release 12.1(19)E:

- If approximately 2000 or more VLAN interfaces are configured in the startup configuration file, the switch might take at least 10 minutes to boot up. The switch is unresponsive until it completes the boot.

  Workaround: Configure fewer switch virtual interfaces (SVIs) in the startup configuration file. (CSCdx91258)

- If you disable IGMP snooping with a large number of groups and VLANs, CPU HOG and HOST FLAPPING messages might be displayed. The following similar messages will appear:

```
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)

- 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 the 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)

- When the WS-X4148-RJ45V module is plugged into a Catalyst 4500 chassis, the Power LED does not work. This caveat is present in 12.1(13)EW and all previous software releases.

  Workaround: None. (CSCdz60995)

- When the fan tray is removed from the switch for more than 5 minutes, the following message is displayed on the console. If the situation persists for 5 minutes, all modules are reset.

Error Message `%C4K_CHASSIS-2-INSUFFICIENTFANSDETECTED: Too few working fans, the chassis will overheat`

  Workaround: None. Do not leave chassis operational without fan tray for more than 5 minutes. (CSCdz50817)

- When a fan tray fails or is removed, the supervisor engine status might not register as faulty and the status LED might not turn amber. When the power supply is removed or fails, the supervisor engine status might not register as faulty and the status LED might not turn red.

  Workaround: None. (CSCdz55274)

- When more than 1000 multicast routes are present, null registers may not be sent and Multicast Source Discovery Protocol (MSDP) may fail to advertise an active route (because the ‘A’ flag is not set). This situation occurs on any route that has a ‘-’ in the output of the **show ip mfib** command for the fast-switched packets.

  Workaround: None. (CSCea89330)

- A switch might accept an invalid boot variable even though the file does not exist.

For example, you may want to set a boot variable to point to the cat4000-is-mz.121-12c.EW image, but you mistakenly type the first letter as upper case C instead of as lowercase c (for example, **boot system flash bootflash: Cat4000-is-mz.121-12c.EW**). When you try to reload the switch it will not boot, because the boot variable is pointing to a nonexistent image.

You will not be able to add the correct boot variable, because the software perceives that it already exists and will not add it to the configuration.

Workaround: Remove the invalid boot variable and add the correct one. (CSCeb05517)

- Occasionally, IP Loop Guard places a port in loop-inconsistent state. The port is assigned a designated role and is unable to recover.

  Workaround: Disable or enable the port. (CSCeb06811)

Resolved Caveats in Software Release 12.1(19)E

This section lists resolved caveats in release 12.1(19)E:

- 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.

  Workaround: Cisco has made software available, free of charge, to correct the problem. (CSCdz71127, CSCea02355)

- 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, which will detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the VLAN configuration **shutdown** command and is reenabled using the VLAN configuration **no shutdown** command, any subsequent flooded or multicast packets received on the private VLAN port do not reach all the destinations.

  Workaround: Do not use the VLAN configuration **shutdown** and **no shutdown** commands to disable the VLAN. To disable the VLANs, 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, 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)

- When you enter the **show interface** command for a connected gigaport on the front panel, an unknown duplex mode is displayed with its flowcontrol information.

  Workaround: None. (CSCdz89143)

- Sometimes when the Catalyst 4000 user VLANs are configured, if you delete one VLAN (to create space for a Layer 3 interface) and enter a **no shut** command on the Layer 3 interface, the interface does not forward packets.

  Workaround: Wait at least 5 seconds, and then delete an existing user-configured VLAN and enter the **no shut** command on the Layer 3 physical interface.(CSCdz56613)

- When a Catalyst 4000 Supervisor Engine III is used as an Layer 2 switch and IGMP-snooping is enabled, the switch sends IGMP leave packets with an IP source address of 0.0.0.0. This problem occurs when the supervisor engine is connected to another vendor's Layer 3 switch that rejects the source address.

  Workaround: None. (CSCdz49171)

- When the image is booted from bootflash, the **show version** command does not display the correct image file name; instead, the command displays "bootflash:unknown."

  Workaround: None. (CSCdz89123)

- The type column in the output of the **show interface status** command might show the physical connector type (for example, RJ-45) instead of the interface type (for example, 10/100-TX).

  Workaround: None. (CSCdy80025)

Open Caveats in Software Release 12.1(14)E1

This section lists open caveats in release 12.1(14)E1.

- If approximately 2000 or more VLAN interfaces are configured in the startup configuration file, the switch might take at least 10 minutes to boot up. The switch is unresponsive until it completes the boot.

  Workaround: Configure fewer switch virtual interfaces (SVIs) in the startup configuration file. (CSCdx91258)

- If you disable IGMP snooping with a large number of groups and VLANs, CPU HOG and HOST FLAPPING messages might display. The following similar messages will appear.

```
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, which will detect any BPDUs received on private VLAN trunk ports. (CSCdx62226)

- When a secondary VLAN is disabled using the **shutdown** VLAN configuration command and is reenabled using the **no shutdown** VLAN configuration command, any subsequent flooded or 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. To disable the VLANs, 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 (for example, 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)

- The type column in the output of the **show interface status** command might show the physical connector type (for example, RJ-45) instead of the interface type (for example, 10/100-TX).

  Workaround: None. (CSCdy80025)

- When you enter the **show interface** command for a connected gigaport on the front panel, an unknown duplex mode is displayed and its flow-control information.

  Workaround: None. (CSCdz89143)

- Sometimes when the Catalyst 4000 user VLANs are configured, if you delete one VLAN (to create space for a Layer 3 interface) and enter a **no shut** command on the Layer 3 interface, the interface does not forward packets.

  Workaround: Wait at least 5 seconds, and then delete an existing user-configured VLAN and enter the **no shut** command on the Layer 3 physical interface.(CSCdz56613)

- When the WS-X4148-RJ45V module is plugged into a 4500 chassis, the Power LED does not work. This caveat is present in 12.1(13)EW and all previous software releases.

  Workaround: None. (CSCdz60995)

- When the fan tray is removed from the switch for more than 5 minutes, the following message is displayed on the console. If the situation persists for 5 minutes, all line cards are reset.

Error Message `%C4K_CHASSIS-2-INSUFFICIENTFANSDETECTED: Too few working fans, the chassis will overheat`

Workaround: None. Do not leave chassis operational without fan tray for more than 5 minutes. (CSCdz50817)

- When a fan tray fails or is removed, the supervisor engine status might not register as faulty and the status LED might not turn amber. When the power supply is removed or fails, the supervisor engine status might not register as faulty and the status LED might not turn red.

  Workaround: None. (CSCdz55274)

- When a Catalyst 4000 Supervisor Engine III is used as an Layer 2switch and IGMP-snooping is enabled, the switch sends IGMP leave packets with an IP source address of 0.0.0.0. The problem occurs when the supervisor engine is connected to another vendor's Layer 3 switch that rejects the source address.

  Workaround: None. (CSCdz49171)

- When the image is booted from bootflash, the **show version** command does not display the correct image file name; instead, the command displays "bootflash:unknown."

  Workaround: None. (CSCdz89123)

Resolved Caveats in Software Release 12.1(14)E1

This section lists resolved caveats in release 12.1(14)E1.

- After you configure private VLAN trunks as normal trunks using the **switchport mode trunk** command, they continue to operate as private trunks. 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, enter the **shutdown**, and **no shutdown** commands after configuring the ports as normal trunks. (CSCdy40311)

- On systems with redundant supervisor engines and large and complex configurations, where the system is actively processing the startup-config file, the redundant supervisor may take over from the active supervisor engine in the boot process. If this happens, the following message is displayed on the active supervisor engine:

```
C4K_REDUNDANCY-4-CONFIGSYNCFAIL: Persistent-config Sync to Standby Supervisor
failed
```

The following messages are displayed on the standby supervisor engine:

```
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 802.1x to be enabled on ports that are configured as private VLAN trunks and private VLAN access ports. This configuration may result in unexpected behavior.

  Workaround: Do not configure 802.1x on PVLAN ports. (CSCdy23098)

- The switch crashes when it attempts to set any 64-bit counters using SNMP because the read-only counters are not protected from SNMP writes.

  Workaround: None. (CSCdz37046)

- When your switch reloads, VLAN is not added to the routing table, although the VLAN interface and physical port status are Up/Up. This symptom occurs when spanning tree Portfast is enabled on the port.

  Workaround: To add the VLAN interface to the routing table, either enter the **clear ip route** command **or the shutdown** and the **noshutdown** command on the VLAN interface. (CSCdz46944)

- A Catalyst 4000 Supervisor Engine III or IV may reload when SNMP objects are written to a file using the cbfDefineFileEntry object of CISCO-BULK-FILE-MIB. This caveat is fixed in 12.1(13)EW and all later releases.

  Workaround: None. (CSCdz24084)

- A switch might reload when you perform an “SNMP get” of the VTPCacheMgmtDomain field of an entry in the ciscoCdpMIB if the entry is for a device that does not support VTP (for example, a Cisco 7200).

  Workaround: None. (CSCdz56298)

- Some ports set to autonegotiate on a WS-X4424-GB-RJ45 module might not link up when connected to a device that has disabled auto-mdix.

  Workaround: Enter the **shutdown** and the **shutdown** commands on the port. (CSCdy17476)

- A switch may reload unexpectedly when a physical port interface becomes a member of the port channel. This situation might occur if a routed port channel interface is brought up with the **no shutdown** command, and the all VLANs in the range 1006 to 4094 are in use.

  Workaround: Ensure that some VLANs are available when you enable routed port channels. (CSCdz39541)

- A Cisco 7940 IP phone might not get inline power when connected to a Catalyst 4000 switch running Supervisor Engine III (WS-X4014). The following messages might also be logged as a result of this problem:

Error Message `Nov 15 14:33:22 EST: %C4K_EBM-4-HOSTFLAPPING: Host 00:09:11:3D:7F:FC in vlan 204 is flapping between port Fa5/18 and port Gi1/1`

Error Message `Nov 15 14:33:36 EST: %SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 204 on FastEthernet5/18 VLAN4.`

Error Message `Nov 15 14:33:36 EST: %SPANTREE-2-BLOCK_PVID_PEER: Blocking FastEthernet5/18 on VLAN204. Inconsistent peer vlan.`

Error Message `Nov 15 14:33:36 EST: %SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet5/18 on VLAN4. Inconsistent local vlan.`

Workaround: Apply external power to the phone. (CSCdz34648)

Open Caveats in Software Release 12.1(12c)EW1

This section lists open caveats in release 12.1(12c)EW1.

- 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 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)

- 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 reenabled 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)

- 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

- 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 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 6 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 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 open caveats in release 12.1(12c)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)

- 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 resolved caveats in release 12.1(12c)EW.

- A Catalyst 4006 switch with Supervisor Engine III using 12.1(11b)EW may 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: Don't 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)

- 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 can 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 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

- 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 12.1(11b)EW may 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: Don't 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)
- 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

- 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

- 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 12.1(11b)EW may 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: Don't 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

- 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

- 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

- 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

- 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 4006 with Supervisor Engine III:

Recovering from Loss of the Boot Loader Image

If you lose the boot loader image, you can recover by using one of the following methods:

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(14)E1, and 12.1(19)E. 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 *Cisco IOS Catalyst 4000 Family 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. 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 *Cisco IOS Software Configuration Guide for the Catalyst 4000 Family Switch*.
- 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 4000 family 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(19)E

None. This is an E train release.

Documentation Updates for Release 12.1(14)E1

None. This is an E train release.

Documentation Updates for Release 12.1(12c)EW

This section describes updates to the Catalyst 4000 family switch documentation. These updates will be included in the next iteration of the documentation.

Changes

This section describes last-minute changes to the Catalyst 4000 family switch documentation.

Cisco IOS System Message Guide for the Catalyst Family Switch

Error Message `C4K_REDUNDANCY-5-CONFIGSYNC:The [char] has been successfully synchronized to the standby supervisor`

Explanation The configuration has been successfully synchronized to the standby supervisor. `[char]` can be either private configuration or startup configuration.

Recommended Action This is an informational message. No action is required.

Cisco IOS Command Reference for the Catalyst 4000 Family Switch

- On pages 2-190 and 191:

Examples This example shows how to display the DHCP snooping binding entries for a switch:

```
Switch# show ip dhcp snooping binding

MacAddress      IP Address     Lease (seconds)     Type       VLAN     Interface
-----------     -----------    ----------------    -----      -----    ------------
0000.0100.0201   10.0.0.1         1600                dynamic     100       FastEthernet3/1
Switch#
```

This example shows how to display a DHCP snooping binding entries IP address:

```
Switch# show ip dhcp snooping binding 172.100.101.102

MacAddress      IP Address       Lease (seconds)     Type       VLAN     Interface
-----------     -----------      ----------------    -----      -----    ------------
0000.0100.0201    172.100.101.102   1600                dynamic     100       FastEthernet3/1
Switch#
```

This example shows how to display the DHCP snooping binding entries MAC address:

```
Switch# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f

MacAddress          IpAddress        Lease(sec)  Type     VLAN  Interface
------------------  ---------------  ----------  -------  ----  --------------------
00:02:B3:3F:3D:5F   55.5.5.2         492         dynamic  99    FastEthernet6/36
Switch#
```

This example shows how to display the DHCP snooping binding entries MAC address for a specific VLAN:

```
Switch# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f vlan 99

MacAddress          IpAddress        Lease(sec)  Type     VLAN  Interface
------------------  ---------------  ----------  -------  ----  --------------------
00:02:B3:3F:3D:5F   55.5.5.2         479         dynamic  99    FastEthernet6/36
Switch#
```

This example shows how to display dynamic DHCP snooping binding entries:

```
Switch# show ip dhcp snooping binding dynamic

MacAddress      IP Address     Lease (seconds)     Type       VLAN     Interface
-----------     -----------    ----------------    -----      -----    ------------
0000.0100.0201   10.0.0.1         1600                dynamic     100       FastEthernet3/1
Switch#
```

This example shows how to display DHCP snooping binding entries on VLAN 100:

```
Switch# show ip dhcp snooping binding vlan 100'

MacAddress      IP Address     Lease (seconds)     Type       VLAN     Interface
-----------     -----------    ----------------    -----      -----    ------------
0000.0100.0201   10.0.0.1         1600                dynamic     100       FastEthernet3/1
Switch#
```

This example shows how to display DHCP snooping binding entries on Ethernet interface 0/1:

```
Switch# show ip dhcp snooping binding interface FastEthernet3/1

MacAddress      IP Address     Lease (seconds)     Type       VLAN     Interface
-----------     -----------    ----------------    -----      -----    ------------
0000.0100.0201   10.0.0.1         1600                dynamic     100       FastEthernet3/1
Switch#
```

- The following line on Table 2-7 on page 2-102

  Arp-Non-Ipv4; 0x0806 and protocol header of Arp is other than 0x0800

- The following line in the Command History section for the **power redundancy-mode** command on page 2-10:

  Support for this command was introduced on the Catalyst 4000 family switch. (4500 Series only:4503, 4506, and 4507)

Cisco IOS Software Configuration Guide for the Catalyst 4000 Family Switch

- First paragraph under Enabling Uplinkfast on page 11-13:

  UplinkFast increases the bridge priority to 49,152 and adds 3000 to the spanning tree port cost of all interfaces on the switch, making it unlikely that the switch will become the root switch. The *max_update_rate* value represents the number of multicast packets transmitted per second (the default is 150 packets per second [pps]).

- Example output for the **show ip dhcp snooping** command on page 17-4:

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled.
DHCP Snooping is configured on the following VLANs:
    10 30-40 100 200-220
Insertion of option 82 information is enabled.
Interface           Trusted        Rate limit (pps)
---------           -------        ----------------
FastEthernet2/1     yes            10
FastEthernet3/1     yes            none
GigabitEthernet1/1  no             20
Switch#
```

Additions

This section lists last-minute additions to the Catalyst 4000 family switch documentation.

Cisco IOS System Message Guide for the Catalyst Family Switch

Error Message `C4K_IOSMODPORTMAN-2-INLINEPOWEROFF:Inline power to the switch has been turned off`

Explanation Software has detected that the passthrough current is disabled. This will cause all phones drawing inline power from the switch to be powered off.

Error Message `C4K_IOSMODPORTMAN-4-INLINEPOWERRESTORED:Resuming normal phone operation since inline power has been restored`

Explanation The inline power supply to the switch has been restored and normal phone operation will resume.

Error Message `C4K_IOSSYSMAN-3-OUTOFPACKETHEADERS:Cannot allocate buffer for a packet header`

Explanation The system cannot allocate a buffer for the packet header.

Recommended Action Call Cisco TAC and be ready to provide the configuration information for the switch.

Error Message `C4K_SUPERVISOR-2-MUXBUFFERNOTPRESENT:Mux buffer (WS-X4K-MUX) [dec] is not present`

Explanation The WS-X4K-MUX line card is either not connected to the backplane properly or is not present. If the line card present in this slot cannot be identified, its SEEPROM cannot be read and it will be unusable.

Recommended Action Return the backplane to Cisco for repair.

Error Message `C4K_SUPERVISOR-3-RETIMERDISABLEFAILED:Failed to disable the retimer of the active supervisor's uplink.`

Explanation The retimer on the active supervisor could not be initialized. In a redundant system, you might see packets transmitted out the active supervisor's non-active uplink. To prevent this, disconnect the second uplink on the active supervisor.

Error Message `C4K_SUPERVISOR-3-RETIMERINITFAILED:Failed to initialize the retimer of the active supervisor's uplink.`

Explanation The retimer on the active supervisor could not be initialized. In a redundant system, you might see packets transmitted out the active supervisor's non-active uplink. To prevent this, disconnect the second uplink on the active supervisor.

Error Message `C4K_IOSMODPORTMAN-4-POWERSUPPLYINSERTED:Power Supply [dec] has been inserted`

Explanation This informational message indicates that the power supply has been inserted. No action is required.

Error Message `C4K_IOSMODPORTMAN-4-POWERSUPPLYREMOVED:Power Supply [dec] has been removed`

Explanation This informational message indicates that the power supply has been removed. No action is required.

Error Message `C4K_REDUNDANCY-5-CONFIGSYNC_RATELIMIT:The [char] has been successfully synchronized to the standby supervisor`

Explanation The configuration has been successfully synchronized to the standby supervisor. This is a rate limited message. These messages are logged at 1 minute intervals, rather than continuously as with many other messages.

Recommended Action This is an informational message. No action is required.

Error Message `C4K_SUPERVISOR-4-OTHERSUPERVISORACTIVEDEBOUNCE:Other supervisor is still holding hardware lock`

Explanation This condition is detected when the redundancy register incorrectly indicates that the other supervisor is holding a lock, and is probably caused by hardware signal latency. Unless there is a real hardware failure, the switch will automatically recover from this state. If there is a persistent hardware failure this message will appear four times.

Error Message `C4K_COMMONHWACLMAN-4-FAILEDTOSWITCHPORTTAGS:Failed to switch port tags, old tag: [object-info] new tag: [object-info]. Software paths: [dec] Hardware paths: [dec]`

Explanation Software failed to switch tags. This could be a transient error. The ACL that we were trying to configure will not become active.

Recommended Action Detaching and attaching ACLs (and policies) again might solve the problem.

Error Message `C4K_COMMONHWACLMAN-4-FAILEDTOSWITCHVLANTAGS:Failed to switch vlan tags, old tag: [object-info] new tag: [object-info]. Software paths: [dec] Hardware paths: [dec]`

Explanation Software failed to switch tags. This could be a transient error. The ACL that you were trying to configure will not become active.

Recommended Action Detaching and attaching ACLs (and policies) might solve the problem.

Cisco IOS Command Reference for the Catalyst 4000 Family Switch

- The following commands were not documented in the current release:
  - show platform cpupacketman
  - show platform cpuport
  - show platform software interface all
  - show platform hardware interface all
  - show platform software drop-port
- Usage guidelines for the **mac access-list extended** command on page 2-102
  - **Note:** MAC ACLs do not match IPv4 ARP packets.
  - **Note:** Appletalk ARP packets do not match Arp-Non-Ipv4 protocol-family. Appletalk ARP packets use Ethertype 0x80F3 and protocol-family Appletalk can be used to match AARP (appletalk arp).

Cisco IOS Software Configuration Guide for the Catalyst 4000 Family Switch

- Under "VLAN Map Configuration Guidelines" on page 21-9:

  Note: VLAN maps do not filter IPv4 ARP packets.
- Under "Configuring Named MAC Extended ACLs" on page 21-8:

  This example shows how to create and display an access list named mac1, denying only EtherType DECnet Phase IV traffic, but permitting all other types of traffic.

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)# deny any any decnet-iv (old) protocol-family decnet (new)
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch # show access-lists
Extended MAC access list mac1
    deny   any any decnet-iv (old) protocol-family decnet (new)
    permit any any
```

Deletions

This section describes last-minute deletions to the Catalyst 4000 family switch documentation.

Cisco IOS System Message Guide for the Catalyst Family Switch

Error Message `C4K_IOSSYSMAN-3-OUTOFPRIVATEPOOLPACKETS:Cannot allocate Gsg packet buffer (probably packet leak)`

Cisco IOS Command Reference for the Catalyst 4000 Family Switch

- The following line on Table 2-7:

  ArpIpv4 - 0x0806 and protocol header of Arp is 0x0800(Ipv4)

Cisco IOS Software Configuration Guide for the Catalyst 4000 Family Switch

- The following lines on Table 25-4:
  - Catalyst 4000 Access Gateway Module with IP/FW IOS (WS-X4604-GWY)
  - Catalyst 4003 and 4006 Layer 3 Services Module (WS-X4232-L3)

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

  m
- 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 *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

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

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

Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Release 12.1(19)E