Release Notes for Catalyst 4500 Series Switch Cisco IOS Release 12.1E

Current Release
12.1(26)E3—August 22, 2005

Previous Releases
12.1(26)E2, 12.1(26)E1,, 12.1(26)E, 12.1(23)E4, 12.1(23)E3, 12.1(23)E1, 12.1(23)E, 12.1(22)E6, 12.1(22)E2, 12.1(20)E6, 12.1(20)E3, 12.1(20)E, 12.1(19)E, 12.1(14)E1

Product Numbers:

- S4KL3-12126E3—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(26)E3
- S4KL3E-12126E3—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(26)E3
- S4KL3-12126E2—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(26)E2
- S4KL3E-12126E2—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(26)E2
- S4KL3-12126E1—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(26)E1
- S4KL3E-12126E1—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(26)E1
- S4KL3-12126E—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(26)E
- S4KL3E-12126E—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(26)E
- S4KL3-12123E4—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(23)E4
- S4KL3E-12123E4—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(23)E4

CISCO SYSTEMS

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

- S4KL3-12123E3—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(23)E3
- S4KL3E-12123E3—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(23)E3
- S4KL3-12123E1—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(23)E1
- S4KL3E-12123E1—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(23)E1
- S4KL3-12123E—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(23)E
- S4KL3E-12123E—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(23)E
- S4KL3-12122E6—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(22)E6
- S4KL3E-12122E6—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(22)E6
- S4KL3-12122E2—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(22)E2
- S4KL3E-12122E2—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(22)E2
- S4KL3-12120E6—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(20)E6
- S4KL3E-12120E6—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(20)E6
- S4KL3-12120E3—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(20)E3
- S4KL3E-12120E3—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(20)E3
- S4KL3-12120E—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, basic Layer 3 software image (RIP, Static Routes, AppleTalk and IPX), Release 12.1(20)E
- S4KL3E-12120E—Cisco IOS for the Catalyst 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(20)E
- S4KL3-12119E—Cisco IOS for the Catalyst 4500 series switch 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 4500 series switch 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 4500 series switch 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 4500 series switch Supervisor Engine III and IV, enhanced Layer 3 software image including OSPF, IGRP and EIGRP, Release 12.1(14)E1

These release notes describe the features, modifications, and caveats for the Cisco IOS on the Catalyst 4500 series switch. The most current software release is Cisco IOS Release 12.1(26)E3.

Catalyst 4500 Series Switch Cisco IOS Release Strategy

Note Release 12.1(26)E3 is a General-Deployment release candidate, and is the last release in the 12.1E train to receive GSBU maintenance. Customers desiring support for newer features, or for ongoing maintenance, should consider the 12.2(18)EW release train.

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

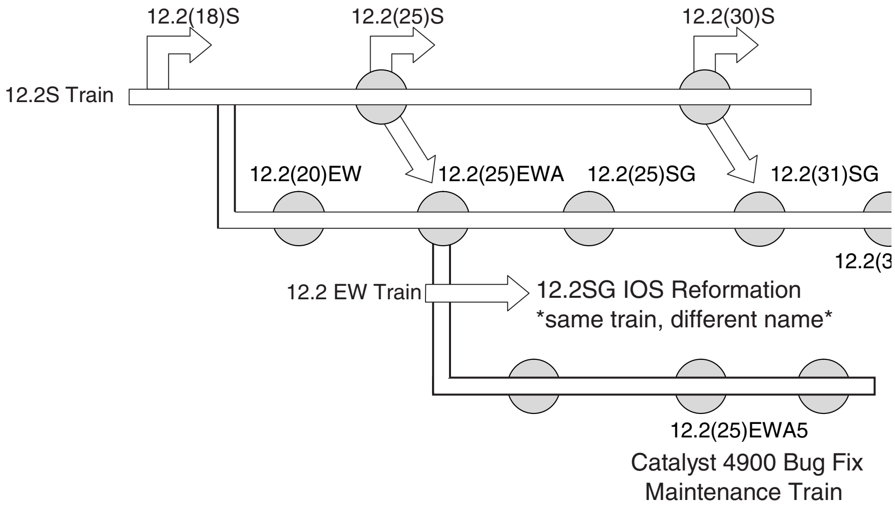
Cisco IOS Software Release 12.2(18)EW1 and all subsequent 12.2(18)EW maintenance releases have only the feature set based on Cisco IOS Release 12.2(18)EW for the Catalyst 4500 Series supervisor engines. Customers with Catalyst 4500 Series supervisor engines who require the stability of a bug fix maintenance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

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

For more information on the Catalyst 4500 series switches, visit the following URL:
www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/index.htm

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

Figure 1 Software Release Strategy



Contents

This publication consists of these sections:

System Requirements

This section describes the system requirements:

- Memory Requirements, page 5
- Supported Hardware, page 5
- Supported Features, page 8
- Unsupported Features, page 10

Memory Requirements

These are the minimum required memory configurations for Cisco IOS software 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 Release**
		Minimum
Supervisor Engines		
WS-X4014=	Catalyst 4500 series switch Supervisor Engine III	12.1(8a)EW
WS-X4515=	Catalyst 4500 series switch Supervisor Engine IV	12.1(12c)EW
WS-X4515/2=	Catalyst 4507R Redundant Supervisor Engine IV	12.1(12c)EW
Gigabit Ethernet Switching Modules		
WS-X4232-GB-RJ	32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	12.1(8a)EW
WS-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-port 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

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
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
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 family Power Entry module	12.1(11b)EW
WS-P4603-2PSU	Catalyst 4000 family Auxiliary Power Shelf (3-slot) including two WS-X4608 power supplies	12.1(11b)EW
WS-X4008-DC	Catalyst 4000 family DC Power Supply	12.1(8a)EW
WS-X4008=	Catalyst 4000 family AC Power Supply	12.1(11b)EW
PWR-C45-1000AC	Catalyst 4500 series switch 1000 Watt AC Power Supply • Data only	12.1(12c)EW
PWR-C45-1300ACV	Catalyst 4500 series switch 1300 Watt AC Power Supply • With integrated voice	12.1(12c)EW
PWR-C45-2800ACV	Catalyst 4500 series switch 2800 Watt AC Power Supply • With integrated voice	12.1(12c)EW

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
Modular Chassis		
WS-C4006	Catalyst 4006 switch chassis: • 1024 MAC addresses • 6 slots • Fan • Redundant supervisor engine-incapable • Supports Supervisor Engine IV, Supervisor Engine III, and Supervisor Engine II	12.1(8a)EW
WS-C4503	Catalyst 4503 switch chassis: • 64 MAC addresses • 3 slots • Fan • Power supply not provided with chassis • Redundant supervisor engine-incapable • Supports Supervisor Engine IV, Supervisor Engine III, and Supervisor Engine II	12.1(12c)EW
WS-C4506	Catalyst 4506 switch chassis: • 64 MAC addresses • 6 slots • Fan • Power supply not provided with chassis • Redundant supervisor engine-incapable • Supports Supervisor Engine IV, Supervisor Engine III, and Supervisor Engine II	12.1(12c)EW
WS-C4507R	Catalyst 4507R switch chassis: • 64 MAC addresses • 7 slots • Fan • Power supply not provided with chassis • Redundant supervisor engine-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
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 48 Mpps
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

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

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
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 version1 and version 2
IGMP filtering
Port Aggregation Protocol (PagP)
SNMP[20] version 1 and version 2
DHCP server and relay agent
DHCP snooping

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

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 feature 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 module and ports 1 thru 12 on the WS-X4412-2GB module

[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(26)E3 for the Catalyst 4500 series switch:

- Bridge groups
- EtherChannel DHCP snooping
  - DHCP snooping on private VLANs
- Cisco IOS software-based transparent bridging (also called “fallback bridging”)
- Secure access through 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 router module
- WS-X4604-GWY access gateway module
- WS-G5483 Cisco 1000BaseT copper GBIC
- Jumbo frames
- IGMP v3 snooping
- DLSw (Data-link switching)
- WCCP (Web Cache Communication Protocol)
- IEEE 802.3ad
- PBR (policy-based routing)
- These 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

There are no new hardware or software features because this is an E train release.

Upgrading the System Software

If you have a Catalyst 4500 series switch running Cisco IOS Release 12.1(11b)EW1 or earlier, and you want to upgrade your switch to Cisco IOS Release 12.1(26)E3, you must upgrade the Supervisor Engine III or Supervisor Engine IV ROMMON version at least to Release 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 12
- Upgrading the Supervisor Engine ROMMON, page 18
- Upgrading the Cisco IOS Software, page 21

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 18, and then upgrade your Cisco IOS software as described in the "Upgrading the Cisco IOS Software" section on page 21.

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 from which you download Catalyst 4500 system images.

Step 2 Download the Cisco IOS Release 12.1(26)E3 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 the **slot0:** command instead of the **bootflash:** command.

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 the 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 installs 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 18) and then upgrade the Cisco IOS software (as described in "Upgrading the Cisco IOS Software" section on page 21).

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 releases. If the ROMMON software or Cisco IOS releases are incorrect, you must upgrade the ROMMON (as described in the "Upgrading the Supervisor Engine ROMMON" section on page 18), and then upgrade the Cisco IOS software (as described in "Upgrading the Cisco IOS Software" section on page 21).

In the following example, the ROMMON release is 12.1(12r)EW, and the Cisco IOS release is 12.1(23)E1:

```
Switch# show version
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-IS-M), Version
12.1(23)E1, 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 the Cisco IOS image cat4000-is-mz.121-14.E1 only:

```
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, read this entire section before starting the upgrade.

If you have a Catalyst 4500 series switch running Cisco IOS Release 12.1(11b)EW1 or earlier, and you want to upgrade your switch to Cisco IOS Release 12.1(26)E3, you must upgrade the Supervisor Engine ROMMON to Release 12.1(12r)EW or higher. When you upgrade and boot the Cisco IOS software to Release 12.1(26)E3, the field programmable gate array (FPGA) is automatically upgraded.

Follow this procedure to upgrade your Supervisor Engine ROMMON to Release 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 series switch 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, and so on, 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 Install and start up Cisco IOS Release 12.1(26)E3 on your switch, and enter the **show version** command to verify that the ROMMON has been upgraded to Release 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 21 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 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 18.

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

Step 1 Download the Cisco IOS Release 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, and so on, 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 release is operating on the switch.

Limitations and Restrictions

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

- For IPX software routing, these features are not supported:
  - NHRP (Next Hop Resolution Protocol)
  - NLSP
- For AppleTalk software routing, these features 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 do not match. If the router with the higher MTU sends a packet larger than the MTU set on the neighboring router, the neighboring router ignores the packet.

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

- Catalyst 4500 series WS-X4124-FX-MT modules with hardware revisions 1.5 and lower are only supported with Supervisor Engine I (WS-X4012) and Supervisor Engine 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, 12.1(19)E, 12.1(20)E, 12.1(20)E3, 12.1(22)E2, 12.1(23)E, 12.1(23)E1, 12.1(26)E, 12.1(26)E1, 12.1(26)E2, and 12.1(26)E3.
- 1q in 1q packet pass-through procedure is supported with the Supervisor Engine III and Supervisor Engine IV, but 1q in 1q encapsulation is not supported with any Catalyst 4500 supervisor engine.
- For PVST and Catalyst 4500 series switch 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.
- Port 1 and port 2 only on the WS-X4418-GB and port 13 and port 14 only 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 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 Releases 12.1(8a)EW, 12.1(11b)EW, and 12.1(12c)EW. (CSCdv20786)
- BGP Conditional Advertisement are not supported in Cisco IOS 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 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 Releases 12.1(8a)EW, 12.1(11b)EW, and 12.1(12c)EW. (CSCdw44274)
- The Unicast Source Discovery Protocol (USDP) cannot support more than 2000 source addresses.

Caveats

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

Open Caveats in Software Release 12.1(26)E3

This section lists open caveats in Release 12.1(26)E3:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all of the trunk ports use VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)
- If approximately 2000 or more VLAN interfaces are configured in the startup configuration file, the switch might take at least 10 minutes to start up. The switch is unresponsive until it completes the backup process. This caveat has been fixed in Release 12.2(18)EW.

  Workaround: Configure fewer switch virtual interfaces (SVIs) in the startup configuration file. (CSCdx91258)
- 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. This caveat has been fixed in Release 12.2(18)EW.

  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(26)E3

This section lists resolved caveats in Release 12.1(26)E3.

- A router may reset its Border Gateway Protocol (BGP) session.

  This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the <CmdBold>bgp maxas limit<noCmdBold> command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log. (CSCeh13489)

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

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

Open Caveats in Software Release 12.1(26)E2

This section lists open caveats in Release 12.1(26)E2:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all of the trunk ports use VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)

- If approximately 2000 or more VLAN interfaces are configured in the startup configuration file, the switch might take at least 10 minutes to start up. The switch is unresponsive until it completes the backup process. This caveat has been fixed in Release 12.2(18)EW.

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

- 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. This caveat has been fixed in Release 12.2(18)EW.

  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(26)E2

This section lists resolved caveats in Release 12.1(26)E2.

- During convergence, a router might stop receiving multicast traffic when a router receives a Join message on an RPF interface and when a downstream router converges faster than the first router.

  In this situation, the router does not populate the RPF interface into the outgoing interface list (OIL) (that is, the OIL remains null) because the old SP-tree has already been pruned by the downstream router. When the RPF interface of the router changes to the new path, it does not trigger a Join message toward the multicast source until the router receives the next periodic Join message from the downstream router and populates the OIL. Consequently, multicast traffic stops temporarily but no longer than the periodic Join message interval.

  Workaround: None. (CSCef60452)

Open Caveats in Software Release 12.1(26)E1

This section lists open caveats in Release 12.1(26)E1:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all of the trunk ports use VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)

- If approximately 2000 or more VLAN interfaces are configured in the startup configuration file, the switch might take at least 10 minutes to start up. The switch is unresponsive until it completes the backup process. This caveat has been fixed in Release 12.2(18)EW.

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

- 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. This caveat has been fixed in Release 12.2(18)EW.

  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(26)E1

This section lists resolved caveats in Release 12.1(26)E1.

- After reloading Supervisor Engine IV, the link does not come up on the non-blocking gigabit ports.

  The serializer/deserializer (SerDes) on the supervisor engine were not initialized correctly, causing the link to fail after a reload. This caveat has been fixed in Releases 12.2(18)EW3, 12.1(26)E1 and 12.2(25)EWA.

  Workaround: None (CSCeg86853).

- Catalyst 4500 supervisor engines running IOS software may spew out log messages such as that displayed below, indicating that the fan-tray failed but the failure recovered within 30 seconds. This caveat might be seen when you use the Catalyst 4507R or 4510R chassis. Traffic is not impacted while these messages display.

```
Dec 21 01:13:46 EST: %C4K_IOSMODPORTMAN-4-FANTRAYBAD: Fan tray has failed
Dec 21 01:13:46 EST: %C4K_CHASSIS-2-INSUFFICIENTFANSDETECTED: Too few working fans in
fan
tray, the chassis will overheat. If not resolved, in 5 minutes all line cards will be
placed into Reset-Mode
Dec 21 01:13:51 EST: %C4K_IOSMODPORTMAN-6-FANTRAYGOOD: Fan tray is okay
Dec 21 01:47:21 EST: %C4K_IOSMODPORTMAN-4-FANTRAYBAD: Fan tray has failed
Dec 21 01:47:21 EST: %C4K_CHASSIS-2-INSUFFICIENTFANSDETECTED: Too few working fans in
fan
tray, the chassis will overheat. If not resolved, in 5 minutes all line cards will be
placed into Reset-Mode
Dec 21 01:47:26 EST: %C4K_IOSMODPORTMAN-6-FANTRAYGOOD: Fan tray is okay
Dec 21 04:00:16 EST: %C4K_IOSMODPORTMAN-4-FANTRAYBAD: Fan tray has failed
Dec 21 04:00:16 EST: %C4K_CHASSIS-2-INSUFFICIENTFANSDETECTED: Too few working fans in
fan
tray, the chassis will overheat. If not resolved, in 5 minutes all line cards will be
placed into Reset-Mode
Dec 21 04:00:21 EST: %C4K_IOSMODPORTMAN-6-FANTRAYGOOD: Fan tray is okay
```

Workaround: None. This is a software bug and the fix is integrated in the releases mentioned for this bug. Do not RMA or EFA the fan-trays. (CSCeg70330)

Open Caveats in Software Release 12.1(26)E

This section lists open caveats in Release 12.1(26)E:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all of the trunk ports use VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)

- If approximately 2000 or more VLAN interfaces are configured in the startup configuration file, the switch might take at least 10 minutes to start up. The switch is unresponsive until it completes the backup process. This caveat has been fixed in Release 12.2(18)EW.

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

- 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. This caveat has been fixed in Release 12.2(18)EW.

  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(26)E

This section lists resolved caveats in Release 12.1(26)E:

- A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command ‘bgp log-neighbor-changes’ configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

If a misformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command ‘show ip bgp neighbors’ or running the command ‘debug ip bgp <neighbor> updates’ for a configured bgp neighbor.

Cisco has made free software available to address this problem.

(CSCee67450)

- When(1) the service policy attached to a port and/or VLAN experiences sustained high traffic and (2) the number of class-maps used in the policy is relatively high (order of 50 - 100 class-maps), the CPU utilization remains high for a long period of time.

  Workaround: None. (CSCeg38623)

- When an interface is configured as a trunk that does not carry VLAN 1, control packets (tagged with VLAN1) that are received on that interface are dropped on ingress. Protocols impacted by this include CDP, PAgP and LACP. This situation impacts Release 12.1(22)E.

  Workaround: Allow the trunk to carry VLAN 1. (CSCee31879)

Open Caveats in Software Release 12.1(23)E4

This section lists open caveats in Release 12.1(23)E4:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all of the trunk ports use VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)

- If approximately 2000 or more VLAN interfaces are configured in the startup configuration file, the switch might take at least 10 minutes to start up. The switch is unresponsive until it completes the backup process. This caveat has been fixed in Release 12.2(18)EW.

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

- 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. This caveat has been fixed in Release 12.2(18)EW.

  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(23)E4

This section lists resolved caveats in Release 12.1(23)E4:

- A router may reset its Border Gateway Protocol (BGP) session.

  This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the <CmdBold>bgp maxas limit<noCmdBold> command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log. (CSCeh13489)

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

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

  (CSCei61732)

Open Caveats in Software Release 12.1(23)E3

This section lists open caveats in Release 12.1(23)E3:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all of the trunk ports use VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)

- If approximately 2000 or more VLAN interfaces are configured in the startup configuration file, the switch might take at least 10 minutes to start up. The switch is unresponsive until it completes the backup process. This caveat has been fixed in Release 12.2(18)EW.

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

- 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. This caveat has been fixed in Release 12.2(18)EW.

  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(23)E3

This section lists resolved caveats in Release 12.1(23)E3:

- On the Catalyst 6500 series switch, policing rate is calcurated lower than configured with small packets(<82bytes). The Catalyst 6500 series switch uses IP length for policing, but these small packets seem to be treated as 82bytes(iplength = 64bytes).

  This symptom is very similar to CSCdx92093, but this happen with nativeIOS.

```
     traffic 1Gbps                        about 256kbps
    -------------> (policing to 256kbps) -------------->
                  +----------------------+
              g1/1|                      |g3/15
smartbits --------|       Cat6509        |------- smartbits
                  |                      |
                  +----------------------+
```

  Workaround: None. (CSCee78451)

Open Caveats in Software Release 12.1(23)E1

This section lists open caveats in Release 12.1(23)E1:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all of the trunk ports use VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)
- If approximately 2000 or more VLAN interfaces are configured in the startup configuration file, the switch might take at least 10 minutes to start up. The switch is unresponsive until it completes the backup process. This caveat has been fixed in Release 12.2(18)EW.

  Workaround: Configure fewer switch virtual interfaces (SVIs) in the startup configuration file. (CSCdx91258)
- 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. This caveat has been fixed in Release 12.2(18)EW.

  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(23)E1

This section lists resolved caveats in Release 12.1(23)E1:

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. (CSCed78149)
- When TCP connections are configured for Path MTU (PMTU) discovery (disabled by default), the connections might be vulnerable to spoofed ICMP packets. A spoofed ICMP packet might cause the TCP connection to use a very low segment size for 10 minutes.

  Workaround: Disable PMTU discovery. (CSCed78149)

- A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

  Cisco will make free software available to address this vulnerability.

  Workarounds, identified below, are available that protect against this vulnerability.

Open Caveats in Software Release 12.1(23)E

This section lists open caveats in Release 12.1(23)E:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all of the trunk ports use VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)

- If approximately 2000 or more VLAN interfaces are configured in the startup configuration file, the switch might take at least 10 minutes to start up. The switch is unresponsive until it completes the backup process. This caveat has been fixed in Release 12.2(18)EW.

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

- 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. This caveat has been fixed in Release 12.2(18)EW.

  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(23)E

This section lists resolved caveats in Release 12.1(23)E:

- Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)
  (CSC65285)

- The packet memory on a Catalyst 4500 series supervisor engine may malfunction. If the packet memory malfunctions, the switch sends data packets with an invalid CRC, and the link partner discards them. Once the problem has been identified by the diagnostics that have been added to detect this problem, the switch automatically shuts down and restarts in “best-effort” mode. In this mode, the affected packet buffers are removed from circulation, and log messages are generated every 30 minutes to alert the user to the failures.

  Workaround: Replace the supervisor engine with packet memory errors. (CSCed61591)

Open Caveats in Software Release 12.1(22)E6

This section lists open caveats in Release 12.1(22)E6:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all of the trunk ports use VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)
- If approximately 2000 or more VLAN interfaces are configured in the startup configuration file, the switch might take at least 10 minutes to start up. The switch is unresponsive until it completes the backup process.

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

Resolved Caveats in Software Release 12.1(22)E6

This section lists resolved caveats in Release 12.1(22)E6:

- None

Open Caveats in Software Release 12.1(22)E2

This section lists open caveats in Release 12.1(22)E2:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all of the trunk ports use VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)
- If approximately 2000 or more VLAN interfaces are configured in the startup configuration file, the switch might take at least 10 minutes to start up. The switch is unresponsive until it completes the backup process.

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

- 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)

Resolved Caveats in Software Release 12.1(22)E2

This section lists resolved caveats in Release 12.1(22)E2:

- Cisco IOS software will fail when you issue the **show platform software interface all** command in Release 12.1(22)E1. Because this command is a permutation of the **show tech-support** command, entering the latter command may also cause the switch to fail.

  Workaround: Avoid using both the **show tech-support** and **show platform software interface all** commands.

  Release 12.1(22)E1 has been deferred for the Catalyst 4500 series switch because of this problem. (CSCee61402)
- Cisco products running Cisco IOS software contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and Cisco IOS Firewall must inspect H.323 messages and might be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  (CSCea46342, CSCin56408, CSCdx40184, CSCec76776, CSCdx76632, and CSCeb78836)
- If you disable IGMP snooping with a large number of groups and VLANs, CPU hog and host flapping messages might be displayed. These 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)
- A network management application that performs an SNMP bulk retrieval of dot1dBridge MIB table entries may timeout on Catalyst 4500 series switches using Cisco IOS Release 12.1(19)EW if the switches contain at least 5000 entries in the Layer 2 MAC address table.

  Workaround: Use the SNMP GetNext command to retrieve the dot1dBridge MIB table entries, and specify a larger timeout value in the network management application. (CSCec02843)
- Traceback occurs when mac-address-table aging-time is configured at its maximum value (1000000 seconds). This traceback does not impact software functionality.

  Workaround: None. (CSCec59154)
- When the WS-X4148-RJ45V module is plugged into a Catalyst 4500 chassis, the power LED does not work. This caveat is present in Cisco IOS Release 12.1(13)EW and all earlier releases.

  Workaround: None. (CSCdz60995)

- When the fan tray is removed from the switch for more than five minutes, the following message displays to warn that the modules will reset in five minutes due to the missing fan tray:

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

  If the situation persists for five minutes, all modules are reset.

  Workaround: Replace the fan tray within five minutes to avoid resetting the modules. (CSCdz50817)

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

  Workaround: None. (CSCdz55274)

- When more than 1000 multicast routes are present, null registers might not be sent, and Multicast Source Discovery Protocol (MSDP) might fail to advertise an active route because the "A" flag is not set. This situation occurs on any route that has a hyphen 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 might 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 an uppercase "C" instead of a 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)

Open Caveats in Software Release 12.1(20)E6

This section lists open caveats in Release 12.1(20)E6:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all the trunk ports carry VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)

- A network management application that performs an SNMP Bulk retrieval of dot1dBridge MIB table entries may timeout on Catalyst 4500 series switches running Cisco IOS Release 12.1(19)EW if the switches contain at least 5000 entries in the Layer 2 MAC address table.

  Workaround: Use the SNMP GetNext request to retrieve the dot1dBridge MIB table entries, and specify a larger timeout value in the network management application. (CSCec02843)

- Traceback occurs when mac-address-table aging-time is configured at its maximum value (1000000 seconds). This Traceback does not impact software functionality.

  Workaround: None. (CSCec59154)

- 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 backup process.

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

- 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)

Resolved Caveats in Software Release 12.1(20)E6

This section lists resolved caveats in Release 12.1(20)E6:

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  - Attacks that use ICMP "hard" error messages
  - Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  - Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. (CSCef60659)

- A document that describes how the Internet Control Message Protocol (ICMP) ould be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a bdevice itself, can be of three types:

  - Attacks that use ICMP "hard" error messages
  - Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  - Attacks that use ICMP "source quench" messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en. (CSCef44225)

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. (CSCsa59600)

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  - Attacks that use ICMP "hard" error messages
  - Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  - Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. (CSCef44699)

- NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

```
cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType                1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot                1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive              1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges       1.3.6.1.4.1.9.9.99999.1.3.4.1.6
```

  (CSCsa81379)

Open Caveats in Software Release 12.1(20)E3

This section lists open caveats in Release 12.1(20)E3:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all the trunk ports carry VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)

- A network management application that performs an SNMP Bulk retrieval of dot1dBridge MIB table entries may timeout on Catalyst 4500 series switches running Cisco IOS Release 12.1(19)EW if the switches contain at least 5000 entries in the Layer 2 MAC address table.

  Workaround: Use the SNMP GetNext request to retrieve the dot1dBridge MIB table entries, and specify a larger timeout value in the network management application. (CSCec02843)

- Traceback occurs when mac-address-table aging-time is configured at its maximum value (1000000 seconds). This Traceback does not impact software functionality.

  Workaround: None. (CSCec59154)

- 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 backup process.

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

- 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)

Resolved Caveats in Software Release 12.1(20)E3

This section lists resolved caveats in Release 12.1(20)E3:

- Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In UserService (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)
  (CSCed65778)

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

  All Cisco products which contain TCP stack are susceptible to this vulnerability. (CSCed27956, CSCed38527, CSCed93836, CSCdz84583, and CSCeb52066)

  vulnerability as it applies to Cisco products that run Cisco IOS® software.

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

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

  This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS). (CSCed68575 and CSCed68573)

- Symptoms: Some Simple Network Management Protocol (SNMP) packets may linger in the input queue while they are processed. However, the packets do exit the queue on their own without any intervention from the user. This fix allows these packets to be removed from the queue more quickly.

  Conditions: This symptom is observed on a device that runs Cisco IOS software and that supports SNMP operations. In addition, the SNMP request must contain a valid community string.

Workaround: Protect the SNMP community strings with good password management. Permit SNMP traffic only from trusted devices. (CSCeb22276)

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

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

  Workaround: Disable IP Inspect and IDS. (CSCed35253)

Open Caveats in Software Release 12.1(20)E

This section lists open caveats in Release 12.1(20)E:

- If switches are connected in a mesh topology, and a topology change occurs, extra sets of BackboneFast packets are sent if all the trunk ports carry VLAN 1. No STP loops occur after the extra BackboneFast packets are sent.

  Workaround: None. (CSCec43960)
- A network management application that performs an SNMP Bulk retrieval of dot1dBridge MIB table entries may timeout on Catalyst 4500 series switches running Cisco IOS Release 12.1(19)EW if the switches contain at least 5000 entries in the Layer 2 MAC address table.

  Workaround: Use the SNMP GetNext request to retrieve the dot1dBridge MIB table entries, and specify a larger timeout value in the network management application. (CSCec02843)
- Traceback occurs when mac-address-table aging-time is configured at its maximum value (1000000 seconds). This Traceback does not impact software functionality.

  Workaround: None. (CSCec59154)
- 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 backup process.

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

Resolved Caveats in Software Release 12.1(20)E

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

- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

- Cisco products running Cisco IOS software contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and Cisco IOS Firewall must inspect H.323 messages and might be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  (CSCea46342, CSCin56408, CSCdx40184, CSCec76776, CSCdx76632, and CSCeb78836)

- 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)

- When the WS-X4148-RJ45V module is plugged into a Catalyst 4500 series switch chassis, the power LED does not work. This caveat is present in Cisco IOS Release 12.1(13)EW and all earlier releases.

  Workaround: None. (CSCdz60995)

- When the fan tray is removed from the switch for more than five minutes, the following message is displayed on the console:

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

  If the situation persists for five minutes, all modules are reset.

  Workaround: None. Do not leave a chassis operational without a 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 become amber. When the power supply is removed or fails, the supervisor engine status might not register as faulty, and the status LED might not become red.

  Workaround: None. (CSCdz55274)

- When more than 1000 multicast routes are present, null registers might not be sent, and Multicast Source Discovery Protocol (MSDP) might fail to advertise an active route because the “A” flag is not set. This situation occurs on any route that has a hyphen 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 might 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 an uppercase “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)

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 series switch chassis, the Power LED does not work. This caveat is present in Release 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:

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

  If the situation persists for 5 minutes, all modules are reset.

  Workaround: None. Do not leave a chassis operational without a 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 might 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 IP version 6 (IPv6) only 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 destinations.

  Workaround: Do not use the VLAN configuration **shutdown** and **no shutdown** commands to disable secondary VLANs. To disable secondary 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 Layer 4 information. Noninitial fragments do not have any Layer 4 information (for example, UDP ports, TCP flag, and so on).

  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 4500 series switch 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 4500 series switch 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 destinations.

  Workaround: Do not use the **shutdown** and **no shutdown** VLAN configuration command to disable secondary VLANs. To disable secondary 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 Layer 4 information. Non-initial fragments do not have any Layer 4 information (for example, UDP ports, TCP flag, and so on).

  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)

- When the Catalyst 4500 series switch 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, sometimes the interface does not forward packets.

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

- When the WS-X4148-RJ45V module is plugged into a Catalyst 4500 series switch chassis, the Power LED does not work. This caveat is present in Release 12.1(13)EW and earlier.

  Workaround: None. (CSCdz60995)

- When the fan tray is removed from the switch for more than five minutes, this message is displayed on the console:

  ```
  %C4K_CHASSIS-2-INSUFFICIENTFANSDETECTED: Too few working fans, the chassis will
  overheat
  ```
  If the situation persists for five minutes, all modules are reset.

  Workaround: None. Do not leave a chassis operational without a 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 4500 series switch Supervisor Engine III is used as a Layer 2 switch, 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 engine might take over from the active supervisor engine in the boot process.

  If this situation occurs, 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 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 might 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, the 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 4500 series switch Supervisor Engine III or Supervisor Engine IV may reload when SNMP objects are written to a file using the cbfDefineFileEntry object of CISCO-BULK-FILE-MIB. This caveat is resolved in Release 12.1(13)EW and later releases.

  Workaround: None. (CSCdz24084)

- A switch might reload when you perform an SNMP Get request 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 switch).

  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 might 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 when 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 4500 series switch with a Supervisor Engine III (WS-X4014). The following messages might be logged as a result of this problem:

```
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

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

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

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)

Troubleshooting

These sections provide troubleshooting guidelines for the Catalyst 4006 with Supervisor Engine III:

- Recovering from Loss of the Boot Loader Image, page 48
- Troubleshooting at the System Level, page 49
- Troubleshooting Modules, page 49
- Troubleshooting MIBs, page 49

Recovering from Loss of the Boot Loader Image

If you lose the boot loader image, you can recover it 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 similar to the BOOTLDR TFTP boot, except for the following:

   – 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 the 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 the boot loader environment is not set by entering the **unset bootldr** command.

c. Set the 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 the 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

The following guidelines are for troubleshooting system-level problems on the Catalyst 4500 series switches:

- 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, 12.1(19)E, 12.1(20)E, 12.1(20)E3, 12.1(22)E2, 12.1(23)E, 12.1(23)E1 12.1(26)E, 12.1(26)E1, and 12.1(26)E2. An Ethernet cable plugged into the Fast Ethernet port is active only in ROMMON mode.

Troubleshooting Modules

The following guidelines are for troubleshooting modules on the Catalyst 4500 series switches:

- When you insert a module into an operating chassis (known as a "hot" insert), 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 4500 Series Module Installation Guide*.
- Whenever you connect an interface that has duplex set to autonegotiate to an end station or another networking device, ensure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the port set to autonegotiate will remain in half-duplex mode, which can cause a duplex mismatch that results in packet loss, late collisions, and line errors on the link.

Troubleshooting MIBs

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

Documentation Updates

Because this is an E train release there are no documentation updates for this and all prior releases on the train.

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, using the Cisco Bug Search Tool (BST), 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.