Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Release 12.2(46)SG1

Current Release
12.2(46)SG1—Sept 15, 2008

Previous Releases
12.2(46)SG

These release notes describe the features, modifications, and caveats for the Cisco IOS software on the Catalyst 4500 series switch. The most current software release is Cisco IOS Release 12.2(46)SG1.

The most current software release is Cisco IOS Release 12.2(46)SG1. The most current release notes for this release is available on Cisco.com at this URL:

http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_release_note09186a00801f5b1e.html

Note Although their *Release Notes* are unique, the 3 platforms (Catalyst 4500, Catalyst 4900 and Catalyst 4900M), use the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide*. Refer to this location:

http://www.cisco.com/go/cat4500/docs

Contents

This publication consists of these sections:

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

Cisco IOS Software Packaging for the Cisco Catalyst 4500 Series

A new Cisco IOS Software package for Cisco Catalyst 4500 Series Switches was introduced in Cisco IOS Software Release 12.2(25)SG . It is a new foundation for features and functionality and provides consistency across all Cisco Catalyst switches. The new Cisco IOS Software release train is designated as 12.2SG.

Cisco IOS Release 12.2(46)SG1 introduces a new LAN Base Software image and an IP upgrade image. These will complement the existing IP Base and Enterprise Services images. The LAN base image is supported on the Supervisor II-Plus-10GE only. It is primarily focused on customers Layer 2 requirements and therefore many of the IP Base features have been removed. If at a later date some of the features are required, the IP upgrade image is available.

The LAN Base image will not support the following features currently offered in the IP Base image ,10Gig Uplinks, FHRP(HSRP/VRRP), GLBP, WCCP, L2PT & QinQ, Netflow, Auto QoS,EIGRP Stub, PIM SM/DM, MLD Snooping, Flex Link, PVST+, RPVST+, EPoE/PoE+, EEM, TDR, SSO,ISSU, CTS and Smartports (Role based Macros).

Orderable Product Numbers:

- S45LB-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE
- S45LBK9-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE. (LAN Base image with Triple Data Encryption Standard (3DES))
- S45IPBU-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE. (IP Base upgrade image)
- S45IPBUK9-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE. (IP Base upgrade image with Triple Data Encryption Standard (3DES))
- S45LB-12246SG=—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE
- S45LBK9-12246SG=—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE. (LAN Base image with Triple Data Encryption Standard (3DES))
- S45IPBU-12246SG=—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE. (IP Base upgrade image)
- S45IPBUK9-12246SG=—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE. (IP Base upgrade image with Triple Data Encryption Standard (3DES))

Catalyst 4500 Series Switch Cisco IOS Release Strategy

Note The release strategy for Release 12.2(46)SG1 matches that of 12.2(46)SG.

Cisco IOS Release 12.2SG 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(46)SG.

Note As part of the Cisco IOS Reformation effort, Cisco IOS Releases 12.2EW and 12.2SG are the same release train with a name change.

Catalyst 4500 Series has two maintenance trains. The Cisco IOS Release 12.2(25)EW train is the most stable train but only has features found in the Cisco IOS Release 12.2(25)EW. The Cisco IOS Release 12.2(31)SG train has more recent features including support for the WS-X4013+10GE supervisor engine. Currently, the Cisco IOS Release 12.2(31)SGA7 is the recommended release for customers desiring a release with a maintenance train.

For more information on the Catalyst 4500 series switches, visit the following URL:

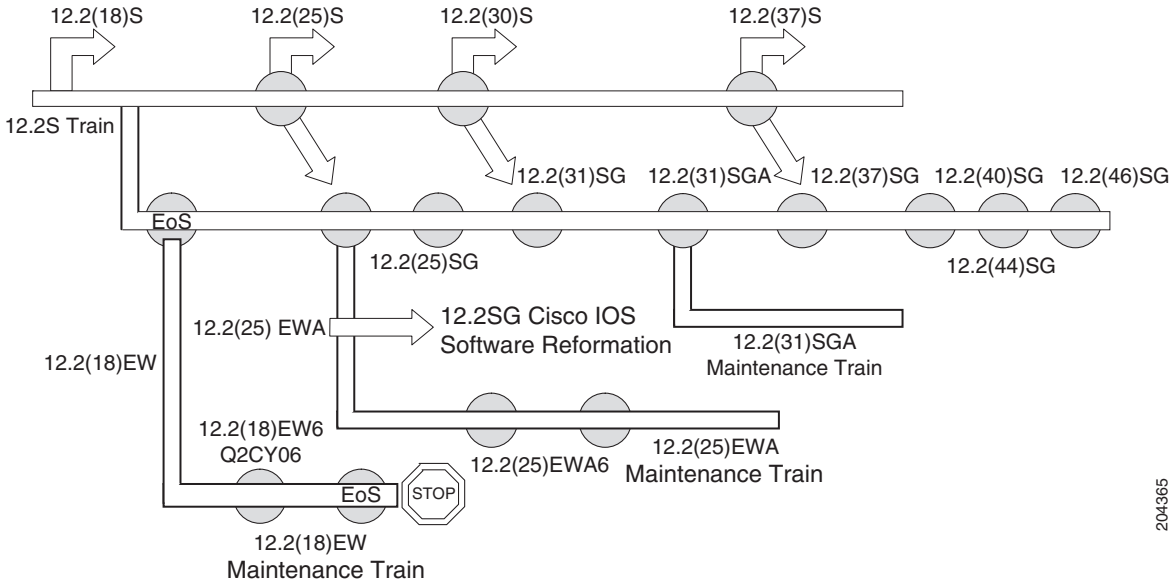
www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/index.htm

Cisco IOS Software Migration Guide

Note Cisco IOS Release 12.2(46)SG1 is a rebuild of Release 12.2(46)SG.

Figure 1 displays the Cisco IOS Software Release 12.2(46)SG plan relative to the 12.2S release train and identifies the recommended migration path. Note that 12.2(44)SG will not be the base release for a new maintenance train. Currently, the Cisco Catalyst 4500 platform has two active maintenance trains: 12.2(25)EWA and 12.2(31)SGA.

Figure 1 Software Release Strategy for the Catalyst 4500 Series Switch



Summary of Migration Plan

Note Cisco IOS Release 12.2(46)SG1 is a rebuild of Release 12.2(46)SG.

- Customers requiring the latest Cisco Catalyst 4500 Series hardware and software features should migrate to Cisco IOS Software Release 12.2(46)SG.
- Cisco IOS Software Release 12.2(31)SGA will continue offering maintenance releases. The latest release from the 12.2(31)SGA maintenance train is 12.2(31)SGA7.
- Cisco IOS Software Release 12.2(25)EWA will continue offering maintenance releases. The latest release from the 12.2(25)EWA maintenance train is 12.2(25)EWA14.

System Requirements

This section describes the system requirements:

- Supported Hardware on Catalyst 4500 Series Switch, page 5
- Supported Features on the Catalyst 4500 Series Switch, page 11
- Unsupported Features, page 12

Supported Hardware on Catalyst 4500 Series Switch

Note The LAN Base image is supported only on the WS-4013+10GE and will support all legacy linecards (not E-Series cards).

Table 1 lists the hardware supported on the Catalyst 4500 Series Switch.

Table 1 Supported Hardware

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
Supervisor Engines		
WS-X4013+10GE	Catalyst 4500 series switch Supervisor Engine II-Plus-10GE	12.2(25)SG
Gigabit Ethernet Switching Modules		
WS-X4302-GB	2-port 1000BASE-X (GBIC) Gigabit Ethernet module	12.1(19)EW
WS-X4306-GB	6-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	12.1(8a)EW
WS-X4418-GB	18-port 1000BASE-X (GBIC) Gigabit Ethernet server switching module	12.1(8a)EW
WS-X4412-2GB-T	12-port 1000BASE-T Gigabit Ethernet and 2-GBIC ports switching module	12.1(8a)EW
WS-X4424-GB-RJ45	24-port 10/100/1000BASE-T Gigabit Ethernet RJ-45 switching module	12.1(8a)EW
WS-X4448-GB-LX	48-port 1000BASE-LX (small form-factor pluggable) Gigabit Ethernet fiber optic interface switching module	12.1(8a)EW
WS-X4448-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet switching module	12.1(8a)EW
WS-X4448-GB-SFP	48-port 1000BASE-X (small form-factor pluggable) module	12.2(20)EW
WS-X4506-GB-T	6-port Alternately-Wired 10/100/1000BASE-T Catalyst 4500 series Power over Ethernet (PoE) 802.3af or 1000BASE-X SFP	12.2(20)EWA
WS-X4524-GB-RJ45V	24-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af	12.2(18)EW
WS-X4548-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet module	12.1(19)EW
WS-X4548-GB-RJ45V	48-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af	12.2(18)EW
Fast Ethernet Switching Modules		
WS-X4124-FX-MT	24-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module	12.1(8a)EW
WS-X4148-FX-MT	48-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module	12.1(8a)EW
WS-X4148-FE-LX-MT	48-port 100BASE-LX10 Fast Ethernet MT-RJ single-mode fiber switching module	12.1(13)EW
WS-X4148-FE-BD-LC	48-port 100BASE-BX10-D module	12.2(18)EW

Table 1 Supported Hardware (continued)

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
WS-X4248-FE-SFP	48-port 100BASE-X SFP switching module	12.2(25)SG
WS-U4504-FX-MT	4-port 100BASE-FX (MT-RF) uplink daughter card	12.1(8a)EW
Ethernet/Fast Ethernet (10/100) Switching Modules		
WS-X4124-RJ45	24-port 10/100 RJ-45 module	12.2(20)EW
WS-X4148-RJ	48-port 10/100 RJ-45 switching module	12.1(8a)EW
WS-X4148-RJ21	48-port 10/100 4xRJ-21 (telco connector) switching module	12.1(8a)EW
WS-X4148-RJ45V	48-port Pre-standard PoE 10/100BASE-T switching module	12.1(8a)EW for data support 12.1(11b)EW for data and inline power support
WS-X4224-RJ45V	24-port 10/100BASE-TX RJ-45 Cisco Catalyst 4500 series PoE 802.3af	12.2(20)EW
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-X4248-RJ45V	48-port 10/100BASE-T RJ-45 Cisco Catalyst 4500 series PoE 802.3af	12.2(18)EW
WS-X4248-RJ21V	48-port 10/100 Fast Ethernet RJ-21 Cisco Catalyst 4500 series PoE 802.3af telco	12.2(18)EW
WS-X4232-RJ-XX	32-port 10/100 Fast Ethernet RJ-45 modular uplink switching module	12.1(8a)EW
Small Form-Factor Pluggable 100 Megabit Ethernet Modules		
GLC-FE-100FX	100BASE-FX, 1310 nm wavelength, 2 km over MMF	12.2(25)SG
GLC-FE-100LX	100BASE-LX, 1310 nm wavelength, 10 km over SMF	12.2(25)SG
GLC-FE-100BX-D	100BASE-BX10-D, 1550 nm TX/1310 nm RX wavelength	12.2(25)SG
GLC-FE-100BX-U	100BASE-BX10-U, 1310 nm TX/1550 nm RX wavelength	12.2(25)SG
Small Form-Factor Pluggable Gigabit Ethernet Modules		
GLC-BX-D	1000BASE-BX10-D small form-factor pluggable module For DOM support, see Table 5 on page 10.	12.2(20)EWA
GLC-BX-U	1000BASE-BX10-U small form-factor pluggable module For DOM support, see Table 5 on page 10.bv	12.2(20)EWA
GLC-SX-MM	1000BASE-SX small form-factor pluggable module	12.2(20)EW
GLC-LH-SM	1000BASE-LX/LH small form-factor pluggable module	12.2(20)EW
GLC-ZX-SM	1000BASE-ZX small form-factor pluggable module	12.2(20)EW
GLC-T	1000BASE-T small form-factor pluggable module	12.2(20)EW
CWDM-SFP-xxxx	CWDM small form-factor pluggable module (See Table 2 on page 8 for a list of supported wavelengths.) For DOM support, see Table 5 on page 10.	12.2(20)EW
10 Gigabit Ethernet X2 Pluggable Modules		

Table 1 Supported Hardware (continued)

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
X2-10GB-LR	10GBASE-LR X2 transceiver module for SMF, 1310-nm wavelength, SC duplex connector	12.2(25)EW
X2-10GB-ER	10GBASE-ER X2 transceiver module for SMF, 1550-nm wavelength, SC duplex connector	12.2(25)EWA
X2-10GB-CX4	10GBASE-CX4 X2 transceiver module for CX4 cable, copper, Infiniband 4X connector	12.2(25)EWA
X2-10GB-LX4	10GBASE-LX4 X2 transceiver module for MMF, 1310-nm wavelength, SC duplex connector	12.2(25)EWA
X2-10GB-LRM	10GBASE-LRM X2 transceiver module for MMF, 1310-nm wavelength, SC duplex connector	12.2(31)SGA
X2-10GB-SR	10GBASE-SR X2 transceiver module for MMF, 850-nm wavelength, SC duplex connector	12.2(25)EWA
Gigabit Interface Converter		
WS-G5483=	1000BASE-T GBIC	12.1(13)EW
WS-G5484	1000BASE-SX short wavelength GBIC (multimode only)	12.1(8a)EW
WS-G5486	1000BASE-LX/LH long-haul GBIC (single mode or multimode)	12.1(8a)EW
WS-G5487	1000BASE-ZX extended reach GBIC (single-handed)	12.1(8a)EW
CWDM-GBIC-xxxx	CWDM gigabit interface converter (See Table 2 on page 8 for a list of supported wavelengths.)	12.1(12c)EW
DWDM-GBIC-xx.yy	Dense Wavelength-Division Multiplexing ITU 100-Ghz grid 15xx.yy nm GBIC. For DOM support, see Table 5 on page 10.	12.1(19)EW
WDM-GBIC-REC	Receive-only 1000BASE-WDM GBIC	12.1(19)EW
Other Modules		
MEM-C4K-FLD64M	Catalyst 4500 series switch CompactFlash, 64 MB Option	12.1(8a)EW
MEM-C4K-FLD128M	Catalyst 4500 series switch CompactFlash, 128 MB Option	12.1(8a)EW
WS-X4590=	Catalyst 4500 series switch Fabric Redundancy Modules	12.2(18)EW
PWR-C45-1000AC	Catalyst 4500 series switch 1000 Watt AC power supply for chassis 4503, 4506, and 4507R (data only)	12.1(12c)EW
PWR-C45-1400DC	Catalyst 4500 series switch 1400 Watt DC triple input power supply (data-only)	12.2(25)EW
PWR-C45-1400DC-P	Catalyst 4500 series switch 1400 Watt DC power supply with integrated PEM	12.1(19)EW
PWR-C45-1400AC	Catalyst 4500 series switch 1400 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 for chassis 4503, 4506, and 4507R	12.1(12c)EW

Table 1 Supported Hardware (continued)

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
PWR-C45-2800ACV	Catalyst 4500 series switch 2800 Watt AC power supply with integrated voice (data and PoE) for chassis 4503, 4506, and 4507R	12.1(12c)EW
PWR-C45-4200ACV	Catalyst 4500 series switch 4200 Watt AC dual input power supply with integrated voice (data and PoE)	12.2(25)EWA5
WS-P4502-1PSU	Catalyst 4500 series switch auxiliary power shelf (25-slot), including one PWR-4502	12.1(19)EW
PWR-4502	Catalyst 4500 series switch auxiliary power shelf redundant power supply	12.1(19)EW

Table 2 briefly describes the supported wavelengths in the Catalyst 4500 Classic Series Switch.

Table 2 CWDM GBIC and SFP Supported Wavelengths for the Catalyst 4500 Classic Series Switch

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
CWDM-GBIC (or SFP) -1470	Longwave 1470 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1490	Longwave 1490 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1510	Longwave 1510 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1530	Longwave 1530 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1550	Longwave 1550 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1570	Longwave 1570 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1590	Longwave 1590 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1610	Longwave 1610 nm laser single-mode	12.1(12c)EW

Table 3 briefly describes the seven chassis in the Catalyst 4500 Series Switch. For the chassis listed in the table, refer to Table 4 on page 10 for software release information.

Table 3 Chassis Description for the Catalyst 4500 Series Switch

Product Number (append with "=" for spares)	**Description of Modular Chassis**
WS-C4503	Catalyst 4503 chassis includes these components: • 3 slots • Fan tray • Supports Supervisor Engine 6-E, Supervisor Engine V-10GE, Supervisor Engine V, Supervisor Engine IV, Supervisor Engine III, Supervisor Engine II-Plus-10GE, Supervisor Engine II-Plus-TS, Supervisor Engine II-Plus, and Supervisor Engine II
WS-C4506	Catalyst 4506 chassis includes these components: • 6 slots • Fan tray • Supports Supervisor Engine 6-E, Supervisor Engine V-10GE, Supervisor Engine V, Supervisor Engine IV, Supervisor Engine III, Supervisor Engine II-Plus-10GE, Supervisor Engine II-Plus, and Supervisor Engine II
WS-C4507R	Catalyst 4507R chassis includes these components: • 7 slots • Fan tray • Supports Supervisor Engine 6-E, Supervisor Engine V-10GE, Supervisor Engine V, Supervisor Engine IV, Supervisor Engine II-Plus-10GE, and Supervisor Engine II-Plus
WS-C4510R	Catalyst 4510R chassis includes these components: • 10 slots; slot 10 accepts only the Catalyst 4500 series 2-port Gigabit Ethernet line card (WS-X4302-GB with Supervisor Engine V **Note** The Supervisor Engine V-10GE does not have this restriction. • Fan tray • Supports Supervisor Engine 6-E, Supervisor Engine V-10GE and Supervisor Engine V

Table 4 lists the software release information for the Catalyst 4500 Series Switch supervisor engines.

Note LAN Base image is only supported on Supervisor Engine II+10GE.

Table 4 Supervisor Engine Support on the Catalyst 4500 Series Switch

Supervisor Engine	Software Release
	Minimum
Supervisor Engine II	Catalyst operating system software
Supervisor Engine II-Plus	12.1(19)EW
Supervisor Engine II-Plus-TS	12.2(20)EWA
Supervisor Engine II-Plus-10GE	12.2(25)SG
Supervisor Engine IV	12.1(12c)EW
Supervisor Engine V	12.2(18)EW
Supervisor Engine V-10GE	12.2(25)EW
Supervisor Engine 6-E	12.2(40)SG

Table 5 DOM Support on the Catalyst 4500 Series Switch

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

Supported Hardware on Catalyst 4500 E-Series Switch

Note The LAN Base image is only supported on Supervisor Engine II-10GE.

For the chassis listed in the table, refer to Table 6 on page 10 for software release information.

Table 6 Supported E-Series Hardware

Product Number	Description
WS-C4503-E	Cisco Catalyst 4500 E-Series 3-Slot Chassis • Fan tray • No Power Supply
WS-C4506-E	Cisco Catalyst 4500 E-Series 6-Slot Chassis • Fan tray • No Power Supply

Table 6 Supported E-Series Hardware

Product Number	Description
WS-C4507R-E	Cisco Catalyst 4500 E-Series 7-Slot Chassis • Fan tray • No Power Supply • Redudant supervisor engine capability
WS-C4510R-E	Cisco Catalyst 4500 E-Series 10-Slot Chassis • Fan tray • No Power Supply • Redudant supervisor engine capability

Supported Features on the Catalyst 4500 Series Switch

Except for the features listed in Table 7, the LAN Base image supports all the features supported on the IP Base image. For details on those features, see the *Catalyst 4500 Series Switch Software Configuration Guide, Cisco IOS Release 12.2(46).*

Table 7 Features not Supported on the LAN Base Image

Feature
Auto-QoS
CTS
EEM
EIGRP Stub
EPoE/PoE+
FHRP(HSRP/VRRP)
Flex Link
GLBP
ISSU
L2PT
MLD Snooping
Netflow
QinQ
PIM SM/DM
PVST+
RPVST+
Smartports (Role based Macros)
SSO
TDR

Table 7 Features not Supported on the LAN Base Image

Feature
Ten-Gigabit Uplinks
WCCP

Unsupported Features

The following features are not supported in Cisco IOS Release 12.2(46)SG1 for the Catalyst 4500 series switches:

- The following ACL types:
  - Standard Xerox Network System (XNS) access list
  - Extended XNS access list
  - DECnet access list
  - Protocol type-code access list
- ADSL and Dial access for IPv6
- AppleTalk EIGRP (use native AppleTalk routing instead)
- Bridge groups
- Cisco IOS software IPX ACLs:
  - <1200-1299> IPX summary address access list
- Cisco IOS software-based transparent bridging (also called “fallback bridging”)
- Connectionless (CLNS) routing; including IS-IS routing for CLNS. IS-IS is supported for IP routing only.
- DLSw (data-link switching)
- IGRP (use EIGRP instead)
- **isis network point-to-point** command
- Kerberos support for access control
- Lock and key
- NAT-PT for IPv6
- PBR with Multiple Tracking Options
- QoS for IPv6 (QoS for IPv6 traffic) (only applies to Supervisor Engines II thru V-10GE)
- Reflexive ACLs
- Routing IPv6 over an MPLS network
- Two-way community VLANs in private VLANs
- CFM CoS

New and Changed Information

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

New Hardware Features in Release 12.2(46)SG1

Release 12.2(46)SG1 provides the following new hardware for the Catalyst 4500 series switch:

- None

New Software Features in Release 12.2(46)SG1

Cisco IOS Release 12.2(46)SG1 introduces the LAN Base and IP upgrade images:

- S45LB-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE
- S45LBK9-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE. (LAN Base image with Triple Data Encryption Standard (3DES))
- S45IPBU-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE. (IP Base upgrade image)
- S45IPBUK9-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE. (IP Base upgrade imagewith Triple Data Encryption Standard (3DES))
- S45LB-12246SG=—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE
- S45LBK9-12246SG=—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE. (LAN Base image with Triple Data Encryption Standard (3DES))
- S45IPBU-12246SG=—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE. (IP Base upgrade image)
- S45IPBUK9-12246SG=—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine II-Plus-10GE. (IP Base upgrade image with Triple Data Encryption Standard (3DES))

Cisco IOS Release 12.2(46)SG1 is a rebuild of Release 12.2(46)SG.

Upgrading the System Software

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

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

Table 8 Supervisor Engine and Minimum Cisco IOS Release

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

Table 9 Supervisor Engine and Recommended ROMMON Release

Supervisor Engine	Minimum ROMMON Release
IV	12.1(12r)EW
II-Plus	12.1(19r)EW
II-Plus-10GE	12.2(25r)SG
V	12.1(20r)EW1
II-Plus-TS	12.2(20r)EW
V-10GE	12.2(25r)EW
6-E	12.2(40r)SG
ME-X4924-10GE	12.2(25)EW

Table 10 ROMMON Release and Promupgrade Programs

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

Table 10 ROMMON Release and Promupgrade Programs

ROMMON Release	Promupgrade Program
12.2(44r)SG	cat4500-e-ios-promupgrade-122_44r_SG
12.2(44r)SG1	cat4500-e-ios-promupgrade-122_44r_SG1

The following sections describe how to upgrade your switch software:

Guidelines for Upgrading the ROMMON

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

Upgrading the Supervisor Engine ROMMON from the Console

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

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

Follow this procedure to upgrade your supervisor engine ROMMON:

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

 Rom Monitor Program Version 12.1(12r)EW


.
.(output truncated)
.

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

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

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

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

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

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

 Image size = 314.236 KBytes

 Maximum allowed size = 511.75 KBytes


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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configuration register is 0x2102

Switch#
```

The ROMMON has now been upgraded.

See the "Upgrading the Cisco IOS Software" section on page 23 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Supervisor Engine ROMMON Remotely Using Telnet

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

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

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

Step 1 Establish a Telnet session to the supervisor engine.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

config-register to 0x0102.

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

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

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

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

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

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

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

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



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

 Rom Monitor Program Version 12.1(12r)EW

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

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


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


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


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

 Current BOOT file is --- bootflash:cat4000-ios-promupgrade-121_20r_EW1
```

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

 Image size = 314.236 KBytes

 Maximum allowed size = 511.75 KBytes


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

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

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

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

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


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

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

Rommon reg: 0x56000380

Running IOS...

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

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

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

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

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

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

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

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

Configuration register is 0x0102

Switch#
```

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

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

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

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

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

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

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

The ROMMON has now been upgraded.

See the "Upgrading the Cisco IOS Software" section on page 23 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Cisco IOS Software

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

Before you proceed, observe the following rules for hostname:

- Do not expect case to be preserved

  Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, Choosing a Name for Your Computer.
- Must start with a letter and end with a letter or digit.
- Interior characters can only be letters, digits, and hyphens; periods and underscores not allowed.
- Names must be 63 characters or fewer; hostname of fewer than 10 characters is recommended.
- On most systems, a field of 30 characters is used for the host name and the prompt in the CLI. Longer configuration mode prompts may be truncated.

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

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

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

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

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

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

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

```
[OK - 6923388/13846528 bytes]

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

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

The following example shows how to clear the BOOT variable:

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

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

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

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

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

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

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

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

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

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

```
Switch# reload
Rommon reg: 0x2B004180

Upgrading FPGA...

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

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

```
* All rights reserved.                                          *
*                                                              *
****************************************************************

Image size = 483.944 KBytes

Maximum allowed size = 1023.75 KBytes


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

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

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

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

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




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

Rom Monitor Program Version 12.1(12r)EW

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


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

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


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

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

Limitations and Restrictions

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

- For IP Unnumbered, the following are not supported:
  - Dynamic routing protocols
  - Static arp
  - Unnumbered interface and Numbered interface in different VRFs
- For WCCP version 2, the following are not supported:
  - GRE encapsulation forwarding method
  - Hash bucket based assignment method
  - Redirection on an egress interface (redirection out)
  - Redirect-list ACL
- For IPX software routing, the following are not supported:
  - NHRP (Next Hop Resolution Protocol)
  - NLSP
  - Jumbo Frames
- For AppleTalk software routing, the following are not supported:
  - AURP
  - AppleTalk Control Protocol for PPP
  - Jumbo Frames
  - EIGRP
- For the Netflow feature, the following limitations apply:
  - Netflow will not account for control packets, packets that encountered link-level errors, and ARP/RARP packets.
  - The software cache for netflow is fixed – users cannot change the size.
  - The statistical distribution row that displays the distribution across various packet sizes is not available.
- For the PBR feature, the following limitatins apply:
  - Packet length-based matching policies are not supported.
  - IP Precedence, TOS and Qos groups are fixed.
  - ACL/Route-map statistics are not updated.
- IGRP not supported (use EIGRP instead).
- The MAC address table is cleared while you switch between supervisor engines if either the 802.1s or 802.1w Spanning Tree Protocol is configured. To minimize address clearing and subsequent packet flooding, configure the edge ports as **spanning-tree portfast** and the link type as **spanning-tree link-type point-to-point**.
- Routes may not properly be redistributed from one routing protocol to another when NSF is enabled on the switch. The success of the redistribution depends on the order in which the routing protocols converge after an NSF switchover.

Workaround: None

- IP classful routing is not supported; do not use the **no ip classless** command; it will have no effect because only classless routing is supported. The command **ip classless** is not supported because classless routing is enabled by default.
- The Catalyst 4510R switch does not support Supervisor Engines II-Plus, III, and IV. Installing an unsupported supervisor engine will cause unpredictable hardware behavior that cannot be controlled by the software. Using an unsupported supervisor in a redundant slot may cause a supported supervisor in the other slot to malfunction.
- Supervisor Engine II-Plus cannot read a CompactFlash card formatted by Supervisor Engine III or Supervisor Engine IV in a prior release.
- Catalyst 4500 supervisor engines will not be properly initialized if the VLAN configuration in the startup file does not match the information stored in the VLAN database file. This situation might occur if a backup configuration file was used.
- A Layer 2 LACP channel cannot be configured with the spanning tree PortFast feature.
- Netbooting using a boot loader image is not supported. See the "Troubleshooting" section on page 45 for alternatives.
- There is no support for downgrading to Release 12.1(8a)EW1 after running Release 12.1(13)EW (or higher). If you need to downgrade, contact your TAC representative for further instructions, and mention caveat CSCdz59058.
- Be aware of the following standard Cisco IOS software behavior when deploying redundant supervisors in a Catalyst 4507R: while the startup configuration file is being parsed, the configuration file is not applied to hardware that does not exist.

  For example, if the active supervisor engine is in slot 1, and you have configured interface Gig 1/1, the supervisor engine in slot 2 becomes active if you remove the active supervisor engine from the chassis. In addition, while the startup configuration file is being parsed, you will receive an error message indicating that interface GE1/1 is no longer present. This behavior is correct. When the formerly active supervisor engine is reinserted into slot 1, there is no configuration for interface Gig 1/1.

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

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

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

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

  Workaround: Because the problem is caused by mismatched MTUs, the solution is to change the MTU on either router to match the other's MTU.
- You can run .1q-in-.1q packet pass-through with Supervisor Engine III and Supervisor Engine IV, but you can run only .1q-in-.1q encapsulation with a Supervisor Engine II+10GE, Supervisor Engine V, and Supervisor Engine V-10GE.
- For PVST and Catalyst 4500 E-Series switch VLAN, Cisco IOS Release 12.1(13)EW support a maximum of 3000 spanning tree port instances. If you want to use more instances, use MST rather than PVST.

- Only ports 1 and 2 on the WS-X4418-GB module and ports 13 and 14 on the WS-X4412-2GB-T module can be set as ISL trunks.
- The Fast Ethernet port (10/100) on the supervisor module is active in ROMMON mode only.
- If an original packet is dropped due to transmit queue shaping or sharing configurations, a SPAN packet copy can still be transmitted on the SPAN port.
- For all software releases, do not use over 100,000 routes.
- All software releases support a maximum of 16,000 IGMP snooping group entries.
- For all software releases, the CLI contains some commands that are not supported. (CSCdw44274)
- Use the **no ip unreachables** command on all interfaces with ACLs configured for performance reasons.
- Layer 3 path load balancing metrics are not supported in Cisco IOS Releases 12.1(8a)EW, 12.1(11b)EW, 12.1(12c)EW, 12.1(13)EW, 12.1(19)EW, and 12.1(20)EW. (CSCdv10578)
- The threshold for the Dynamic Arp Inspection err-disable function is set to 15 ARP packets per second per interface. You should adjust this threshold depending on the network configuration. The CPU should not receive DHCP packets at a sustained rate greater than 1000 pps.
- A limited number of ACL bindings are dynamically installed by the IP source guard feature on a Catalyst 4500 series switch Supervisor Engine II-Plus. To take full advantage of the IP source guard feature, you should use the Catalyst 4500 series switch Supervisor Engine IV.
- If you first configure an IP address or IPv6 address on a Layer 3 port, then change the Layer 3 port to a Layer 2 port with the **switchport** command, and finally change it back to a Layer 3 port, the original IP/IPv6 address is lost.
- By default, IPv6 is not enabled. To route IPv6, you must enter the **IPv6 unicast-routing** command. If you plan to use IPv6 multicast routing, use the **IPv6 multicast-routing** command.
- By default, CEF is not enabled for IPv6 (after IPv6 unicast routing is enabled). To prevent IPv6 traffic from being process-switched, use the **IPv6 cef** command.
- Multicast sources in community VLANs are not supported.
- Two-way community VLANs are not supported.
- Voice VLANs are not supported on community VLAN host interfaces.
- Private VLAN trunks do not carry community VLANs.
- When you use private VLANs on the WS-4516 module, old ARP entries will not timeout of the ARP cache if you do not manually clear the entry. This event has no affect on production.
- Compact flash formatted in Cisco IOS Release 12.2(20)EW should be re-formatted in release 12.2(25)EW on both Supervisor Engine V-10GE and non-Supervisor V-10GE systems. Compact flash formatted on any other release need not be re-formatted on non-Supervisor Engine V-10GE systems.
- In a redundant system, do not remove and reinsert the standby supervisor while the active supervisor is booting up. Doing so may cause a failure in the online diagnostics test.

  Workaround: Remove and reinsert the standby supervisor after the active supervisor boots. (CSCsa66509)
- Slot 10 of the Supervisor Engine V accepts only the Catalyst 4500 series two-port Gigabit Ethernet line card (WS-X4302-GB).

- The maximum number of unique private VLAN pairs supported by the **switchport private-vlan mapping trunk** command above is 500. For example, one thousand secondary VLANs could map to one primary VLAN, or one thousand secondary VLANs could map *one to one to one thousand* primary VLANs.
- Support for PoE depends on the use of line cards and power supplies that support PoE.

  PoE switching modules:

  - WS-X4148-RJ45V
  - WS-X4224-RJ45V
  - WS-X4248-RJ45V
  - WS-X4248-RJ21V
  - WS-X4524-GB-RJ45V
  - WS-X4548-GB-RJ45V

  PoE enabled power supplies:

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

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

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

  Workaround: Disable idle timeouts. (CSCec30214)

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

  Workarounds:

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

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

- IPSG for Static Hosts supports the same port mode as IPSG except that it does not support trunk port:
  - It supports Layer 2 access port and PVLAN host port (isolated or community port).
  - It does not support trunk port, Layer 3 port, or EtherChannel.
- IPSG for Static Hosts should not be used on uplink ports.
- Selective DBL is only supported for non-tagged or single-tagged IP packets. To achieve Selective DBL-like functionality with a non-IP packet (like Q-in-Q and IPX), apply an input policy map that matches COS values and specifies DBL in the class map.
- For Selective DBL, if the topology involves Layer 2 Q in Q tunneling, the match cos policy map will apply to the incoming port.
- If a set of DSCP values are already configured (for example, 0-30, 0-63), specifying a subset of these DSCP values with the **qos dbl dscp-based 0-7** command will not remove the unwanted DSCP values of 8 through 63. Rather, you must use the **no** form of the command to remove the extraneous values. In this case, the **no qos dbl dscp-based 8-63** command will leave 0-7 selected.
- If policing is performed on an input policy, the DBL used in output policies for the flow is ignored. (CSCsh60214)
- When you use Port Security with Multi Domain Authentication (MDA) on an interface:
  - Allow for at least three MAC addresses to access the switch: two 2 for the phone (the MAC address of a phone gets registered to the Data domain and Voice domain), and one for the PC.
  - Ensure that the data and voice VLAN IDs differ.
- For IP Port Security (IPSG) for static hosts, the following apply:
  - As IPSG learns the static hosts on each interface, the switch CPU may hit 100 percent if there are a large number of hosts to learn. The CPU usage will drop after the hosts are learned.
  - IPSG violations for static hosts are printed as they occur. If multiple violations occur simultaneously on different interfaces, the CLI displays the last violation. For example, if IPSG is configured for 10 ports and violations exist on ports 3, 6, and 9, the violation messages are printed only for port 9.
  - Inactive host bindings will appear in the device tracking table when either a VLAN is associated with another port or a port is removed from a VLAN. So, as hosts are moved across subnets, the hosts appear in the device tracking table as INACTIVE.
  - Autostate SVI does not work on EtherChannel.
- With the resolution of CSCsg08775, a GARP ACL entry is no longer part of the Static CAM area. However, a system-defined GARP class in Control Plane Policing (CPP) still exists. CPP is a macro with many CLIs and the GARP class creation CLI has been removed.

- As of Cisco IOS Release 12.2(31)SGA1, the GARP class is no longer part of the CoPP. (Due to the fix associated with CSCsg08775, even though the system-cpp-garp-range entry still appears in the CPP configuration, it is merely idling and will be removed in future releases.) Henceforward, you can manipulate GARP traffic with user ACLs and QoS. If you want to protect a CPU against GARP packets, you also can *police down* GARP packets using CoPP after you define the user class for the GARP packet. (This is now possible because GARP is no longer part of the Static CAM area.)

  Because CPP implementation is tightly integrated between IOS and platform code, an error message will always appear during boot-up and CPP will not be applied when you downgrade IOS software from a version where this caveat is integrated to a previous release (where this fix is not present):

  ```
  %Invalid control plane policy-map; Please unconfigure policy-map attached to
  control-plane, and associated class-maps, and execute config command "macro global
  apply system-cpp" error: failed to install policy map system-cpp-policy
  ```

  Workaround:

  1. Backup your configuration when downgrading software.

  2. Remove all CPP entries manually from the configuration and then re-apply the **macro global apply system-cpp** command.

  This caveat should not affect your system while you upgrade between releases (CSCsh45714).

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

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

  Option 1

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

  Option 2

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

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

  Option 1

  Only 4 linecard slots can be used on the Cat4507R and 6 line card slots on the Cat4510R chassis.

  Option 2

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

- When ipv6 is enabled on an interface through any CLI, you might see the following message:

  ```
  % Hardware MTU table exhausted
  ```

In such a scenario, the ipv6 MTU value programmed in hardware is different from the ipv6 interface MTU value. This will happen if there is no room in the hardware MTU table to store additional values.

You must make room in the table by unconfiguring some unused MTU values and subsequently disable/re-enable ipv6 on the interface or reappling the MTU configuration.

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

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

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

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

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

Note The above condition also applies to IPSG with Static Hosts on a PVLAN host port.

- On a Supervisor Engine V-10GE (WS-X4516-10GE) in a 10-slot chassis (Catalyst 4510R and 4510RE), if a startup configuration with a new uplink mode is copied into flash memory and the system is power cycled, the system will not start with the new uplink mode. After you copy the startup configuration with the new uplink mode into flash memory, you must change the uplink mode to the new uplink mode through the command interface before the system is power cycled. This ensures that the system starts in the new uplink mode.
- When the Supervisor Engine V is used in the Catalyst 4510R or 4510R-E chassis, slot 10 (FlexSlot) will only support the following linecards: the two-port GBIC (WS-X4302-GB) and the Access Gateway Module (WS-X4604-GWY). Supervisor Engine V-10GE has this same restriction when its uplink select mode is configured to all. Supervisor Engine V-10GE supports all Catalyst 4500 Series linecards in slot 10 when its uplink select mode is configured to tengigabitethernet or gigabitethernet. Supervisor Engine 6-E supports all Catalyst 4500 series linecards in slot 10.

For Features on the LAN Base Image

Table 11 Features on LAN Base Image

Feature	LAN Base	IP Base
Port Security	1024 MACs	3000 MACs
SPAN	2 ingress sessions and 2 egress sessions	8 sessions bidirectional
Security ACEs	4K	8K
QoS Filters	4K	8K
PoE	Up to 15.4 W	15.4 W, 20 W, and 30 W

Caveats

Note No new bug fixes are introduced in Cisco IOS Release 12.2(46)SG1.

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

Note All caveats in Release 12.4 also apply to the corresponding 12.1 E releases. Refer to the *Caveats for Cisco IOS Release 12.4* publication at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124relnt/124cavs/124mcavs.htm

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

Open Caveats in Cisco IOS Release 12.2(46)SG1

This section lists the open caveats in Cisco IOS Release 12.2(46)SG1:

- None

Resolved Caveats in Cisco IOS Release 12.2(46)SG1

This section lists the open caveats in Cisco IOS Release 12.2(46)SG1:

- None

Open Caveats in Cisco IOS Release 12.2(46)SG

This section lists the open caveats in Cisco IOS Release 12.2(46)SG:

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

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

```
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

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

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

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

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

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

(CSCef01798)

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

  Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  – If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.

  – If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

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

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

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

  This does not affect performance.

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

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

Workaround: Upgrade to Cisco IOS Release 12.2(31)SG or later and resize the TCAM with the **access-list hardware region balance** command to support the ACL Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCse50565)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- If you attempt to downgrade to Cisco IOS Release 12.2(37)SG from Release 12.2(37)SG1 and if the process is started with active supervisor engine in slot-2, the downgrade fails at **runversion**.

  Workaround: None. (CSCsj83688)

- If an Cisco IP Phone has an supplicant attached, upon reloading a DUT port configured with MDA and attached to phones and supplicants, the port will not pass traffic. Phone will in an unknown state.

  Problem is not observed if the phone is a stand alone device.

  Workarounds: Powercycle the Cisco IP phone. (CSCsk81297)

- After a data device is authorized (thru dot1x or MAB) on a port configured with Multi-Domain Authentication (MDA), changing the access VLAN causes traffic loss for this device even if no device is connected on the port. It does *not* affect the traffic from the voice device connected to the port.

  Workaround: Enter the **shutdoown**, then **no shutdown** commands on the interface after changing the access VLAN on the port. (CSCsk45969)

- When traffic is sent on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225ms.

  Workaround: None. (CSCsm30320)

- Manual Pre-emption is disallowed after you modify a set of blocked VLANs with REP and VLAN load balancing configured.

  Workaround: Intentionally fail the link between two switches by physically pulling the cable or shutting down the interface. Then, return the links to a normal condition. This is followed by delayed preemption, which you might have already configured. (CSCsm91997)

- Occasionally, if a PC continues to send traffic behind an 802.1X capable phone that is plugged into a port configured with MDA (Multi-Domain Authentication), MAB (MAC Authentication Bypass) and port security, a 802.1X security violation is triggered if the port observes traffic from the PC before the phone is fully authorized on the port.

  Workaround: Authenticate the phone before plugging a PC behind the phone. (CSCsq92724)

- Ordinarily, the output of a CFM Traceroute from a MEP normally lists the next hop name(device or host name) for each hop until the other MEP. When CFM over EtherChannel exists between the two MEPs, CFM Traceroute entered from a MEP does not show the next hop name.

  Workaround: None. (CSCso50659)

- An IP unnumbered configuration is lost after a reload.

  Workarounds: Do one of the following:

  – After a reload, copy the startup-config to the running-config.

  – Use a loopback interface as the target of the **ip unnumbered** command.

  – Change the CLI configuration so that during bootup the router port is created first.

  (CSCsq63051)

- After CFM is disabled globally and a switch is reloaded with the CFM configuration, and after CFM is enabled globally, CFM are inactive, causing a loss of CFM neighbors.

  Workarounds: Do one of the following:

  – Reapply the CFM configuration; remove and re-add the MEPs configured on all the interfaces of the switch.

  – Deallocate CFM service VLANs. Then reallocate them.

  (CSCsq90598)

- In SSO mode, when a port-channel is created, deleted, and re-created on an active supervisor engine with the same channel-number, the standby port-channel state goes out of sync. After a switch over, the following message displays:

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the portchannel, create a new channel. (CSCsr00333)

Not supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with HWCOPP (HW Control Plane Policing).

  Workaround: None. (CSCso93282)

- CFM packets pass through the Layer 2 protocol tunnel.

  Workaround: None. (CSCsq72572)

- The **show ip cache verbose flow** command does not display the AS path information, when netflow aggregation for origin-as is configured.

  Workaround: None. (CSCsq63572)

Supervisor Engine 6-E Specific

- Software qos does not match a .1Q packet properly for applying the desired qos actions.

  Workaround: None.

  The support to handle .1Q packets for software QoS lookup unavailable in the Cisco IOS Release 12.2(40)SG release. (CSCsk66449)

- When policer or shape or shape values are specified in terms of percentage of link bandwidth on a policy and the interface on which it is attached is forced to a specific speed with the **speed** *10/100/1000* command, the applied policer or shape or bandwidth value might not correspond to the new forced speed.

  Service policy has to be configured with percentage police or shape or share values and the link speed is forced to a specific values. For example

  ```
  Policy-map p1
      class-map c1
         police rate percent 10
  ```

  Workaround: Either use the **speed auto** *10/100/1000* command or the absolute policer, shape or shape values rather than percentage values. For example,

  ```
  Policy-map p1
     class-map c1
       police rate 10 mbps
  ```

(CSCsk56877

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service-policy.

  When an output service-policy is attached to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued to the queue are subjected to the DBL algorithm. If one or more flows are classified as *belligerent* (flows do not back-off in response to drops because of congestion in the queue), those flows continue to be classified as belligerent even when DBL is disabled on that queue.

  For this condition to persist, the transmit queues in question must remain congested for a long period of time and that congestion must be caused by flows that remain belligerent.

  Workaround: Provided the queue in question is non-default (queuing actions are not configured in the class-default class of the policy-map), detach and re-attach the service-policy.

  If this happens on the default queue, modifying and resetting some queuing parameters like bandwidth/shape fixes the issue. (CSCsk62457

- When an E-series switch encounters either a fan tray failure or a supervisor critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

  Workarounds: Use the **show log** command to determine the cause of the power-down.

  – If the log has *LogGalInsufficientFansDetected* messages, the cause was a fan-tray failure.

  – If the log has *LogRkiosModuleShutdownTemp* messages, the cause was that the supervisor critical temperature exceeded the failure threshold.

  (CSCsk48632)

- When two switches are connected back-to-back via two or more links and when a packet is locally-originated, the source IP address may not correspond to the IP address of the outgoing interface. A switch receiving such a packet with unicast RPF feature enabled might drop the incoming packet.

  Workaround: None. (CSCsh99124)

- A Catalyst 4500 series switch with Supervisor Engine 6-E will support a maximum of 32 MTU values system wide.

  On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. Furthermore, MTU values are not retained for modules that are physically moved.

  Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you will observe CRC errors after a reload or power cycle when you insert the card or the X2.

  Workaround: Reinsert the X2. (CSCsk43618)

- Control plane policing applied to DHCP traffic as identified by the system class-maps system-cpp-dhcp-cs, system-cpp-dhcp-sc, and system-cpp-dhcp-ss may not be effective.

  Workaround: None. CSCsk67395)

- When the CPU transmits .1X packet on an interface that has an egress qos policy attached, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original COS value for a .1X packet cannot be matched by software QoS (as per CSCsk66449). The packet is transmitted with whatever COS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured through CSCsk66449, which indicates that the software QoS cannot match against a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, there is no command to check the current operating state.

  Workaround: None. You cannot explicitly check the trusted boundary state. However, you can indirectly determine this state:

  The trusted boundary feature ensures whether the packet's COS/DSCP value will b e trusted or not. When the interface is not in a trusted state, the COS/DSCP fields are forced to zero on a received packet.

  A QoS policy exists on that interface that uses that COS/DSCP value for classification. Therefore, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state. (CSCsh72408)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map command** displays an incorrect burst value.

  Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- Executing **default interface** twice on a port configured with the cisco-phone macro displays the back trace.

  Workaround: Remove the configuration line by line without entering the **default interface** command. (CSCsj23103)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

  Workaround: None. However, if you enter the **show policy-map** *name*, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as "Unknown". After booting IOS, the chassis type is listed properly.

  Workaround: None. (CSCsl72868)

- If you configure a QoS policy with queuing actions (like sharing and shaping) on WS-X4648-RJ45V-E (PoE) and WS-X4648-RJ45V+E (Premium PoE with 30 W per port) line cards, the sharing and shaping percentage error increases to 3 per cent after a SSO switch over.

  Workaround: Do one of the following:

  – Remove the service-policy from the interface and reapply the configuration through the command [**no**] **service-policy** {**input**|**output**}.

  – Enter **shutdown** then **noshutdown**.

  (CSCsm45156)

- When you specify a DBL action for the 'class-default' class-map in a policy-map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. The size range is dictated by the **queue-limit** command. (CSCso06422)

- When IPv4 routes are advertised by RTR2 to RTR3 over IPv6 peering, the first 32 bits of RTR2's IPv6 address is converted to an IPv4 address. This IPv4 address is advertised as the nexthop address to RTR3. If this address results in a Martian address, then RTR3 will ignore the BGP update message, and will not learn the IPv4 routes.

  Configuring an inbound routemap on RTR3 to override the nexthop advertised by RTR2 does not avoid this problem because the BGP update message is ignored.

  Workaround: Configure a n outbound routemap on RTR2 to explicitly set the IPv4 nexthop rather than allow the protocol to derive it implicitly. (CSCsk65139)

- When we try to modify the allocated link bandwidth for IPv6 EIGRP using the **ipv6 bandwidth-percent eigrp as-number percent** command, the supervisor engine reloads. If you enable redundancy, the STANDBY supervisor engine changes to ACTIVE, and the reloaded supervisor engine is set to STANDBY.

  Workaround: None. (CSCso30051)

- Uplinks go down when upgrading the rommon of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

  This behavior occurs in a redundant switch when the ACTIVE supervisor engine is running IOS, the STANDBY supervisor engine is in rommon, and the STANDBY's rommon is upgraded from version 0.34 or to a later version. The upgrade process will cause the uplinks on the STANDBY supervisor engine to go down but the ACTIVE supervisor engine is unaware of this.

  Workarounds: To resume normal operation, do one of the following:

  - Reload both supervisors with the redundancy reload shelf command.
  - Power-cycle the STANDBY supervisor engine by briefly pulling it from the chassis.

    There is *no* workaround for the link flap issue. (CSCsm81875)

- The message "**Module M linecard watchdog has expired**" appears when the switch boots.

  The message may appear when a linecard boots, depending on how the hardware has powered-up.

  Workaround: Reset the linecard. (CSCsq21215)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

  This problem can happen when pause frames are sent to the switchport and the flow control receive configuration is toggled on 10G port.

  Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- IGMP snooping entries are active even after you disable IGMP snooping globally.

  Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally.

  (CSCsq71546)

- Adding and removing the prefix list does not update the IPv6 EIGRP routes.

  Workaround: Enter **shut** followed by **no shut** on the interface to which the prefix list has been added. (CSCsq69116)

- On a Catalyst 4500 series switch running Cisco IOS Release 12.2(47)SG, if you configure the switch port connecting to the AAA server as a Layer 2 interface with SVI enabled on the access VLAN, any MDA (Multi-domain Authentication) port configured with port security and spanning-tree portfast might experience an 802.1X security violation when an 802.1X enabled phone tries to authenticate on the MDA port.

  Workarounds:

  a. Disable port security on the port, or connect the switch to the AAA server through a standard Layer 3 port.

  b. Disable spanning-tree portfast.

  (CSCsq62342)

- Percentage based input policer on an interface with non-default speed doesn't work after the system reloads.

  Workaround: Remove and re-apply the service-policy on the interface.

  (CSCsq79073)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

  The issue is observed only for packets that are logically switched through the switch but are internally controlled such that on egress the system generated by the switch itself. This can happen for certain snooping features like DAI, IGMP snooping, and DHCP snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

  Workaround: None.

  (CSCso96660)

- When policer or shape values are specified as a per cent of link bandwidth on a policy and the interface on which they are attached is forced to a specific speed using the **speed 10/100/1000** command, the applied policer or shape value might correspond to the new forced speed.

  Example:

```
Policy-map p1
       class-map c1
          police rate percent 10
```

  Workaround: Use either the **speed auto 10/100/1000** command or the absolute policer or shape values instead of percentage values.

  Example:

```
Policy-map p1
      class-map c1
        police rate 10 mbps
```

  (CSCsk56877)

- Channel unbundles and re-bundles when a policy map with per cent based actions is shared between channel member ports and another standalone port, and the standalone port is modified from Layer 2 to Layer 3 or Layer 3 to Layer 2.

  Workaround: None. (CSCso54096)

- In SSO mode, when you add, remove, or modify service-policies to port-channel members, you see the following traceback on both the active and standby supervisor engine:

```
03:50:00: %SM-4-BADEVENT: STANDBY:Event 'bundle_sync' is invalid for the current state
'COLLECTING_DISTRIBUTING': lacp_mux Gi7/7 - mux
```

```
-Traceback= 10B97B80 10B98294 10189F78 1038FE0C 103944FC 1055E420 1055C4B8 10A2C28C
10A2AE88 10A2A4B0 10A27A18 10A225E8 1059E824 10595AAC
```

Workaround: None. CSCso23786)

- IPv6 MLD entries are active even if an IPv6 MLD related configuration does not exist.

  Workaround: Unconfigure all generic QOS policies from the system. (CSCsq84853)

- IPv6 entries are active in the CAM; the CPU receives IPv6 packets.

  Workaround: Unconfigure any generic QOS policies from the system. The QoS policies with the **match any** attribute cause IPv6 entries to become active. If the switch is a pure Layer 2 device, remove the generic protocol family attributes and narrow it to the protocol family.

  (CSCsq84796)

- Initially, REP configured with VLAN Load Balancing (VLB) works correctly. When you enter a force-switchover on the switch, that has a port acting as the secondary ALT port, a loop is induced in the topology.

  Workaround: Enter shut, then no-shut on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- The IPv6 ICMP neighbor state changes from **REACH** to **STALE** after 15 secs of inactivity on the link.

  Workaround: Ping the global and link local addresses of the neighbor to ascertain and reinstate reachability. (CSCsq77181)

- IPv6 EIGRP routes are not learned through the port channel.

  Workaround: Unconfigure the port channel and the associated physical port, and reconfigure them.

  (CSCsq74229)

- When a CFM Inward Facing MEP(IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as **Inactive**. Then, you allocate the VLAN, the CC-status remains **Inactive**.

  You only see this symptom if you did not allocate a VLAN before you configure the IFM, then at a later time allocate the same VLAN.

  Workaround: Unconfigure, then reconfigure the IFM on the port.

- With CFM, if the VLAN associated with the service instance/MEP is allocated after the Inward Facing MEP (IFM) is configured on an interface whose status is **down**, the IFM CC status remains **inactive** in the output of the **show ethernet CFM maintenance local** command. Also, the CFM remote neighbor is not seen.

  This behavior is only seen when VLAN is allocated after the IFM is configured.

  Workaround: Unconfigure with the **no ethernet cfm mep level mpid vlan** command, then reconfigure the IFM with the **ethernet cfm mep level mpid vlan** command on the port after the VLAN is allocated. Verify that the C-Status of the IFM is Active with the **show ethernet cfm maintenance-points local** command. (CSCsm85460)

Resolved Caveats in Cisco IOS Release 12.2(46)SG

This section lists the resolved caveats in Release 12.2(46)SG:

- After configuring the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs are seen on the console of the standby supervisor engine:

  ```
  00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum (20000). Dampening is OFF

  00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum 000). Dampening is OFF
  ```

  At this point, if you revert back to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

  Workaround: Enter the **no bgp dampening** command, then the **bgp dampening** command. (CSCse12485)

- The REP Admin VLAN and RSPAN destination VLAN should not match. A given VLAN can be configured as a REP Admin VLAN as well as an RSPAN destination VLAN.

  Workaround: Ensure that the REP Admin VLAN and the RSPAN destination VLAN differ. (CSCso12495)

- Under VLAN Load Balancing, the failure of a segment or the removal of supervisor engine may cause looping in the REP segment.

  Workaround: None. (CSCsm61748)

- Not all combinations of features can be simultaneously supported by the hardware. When such a feature combination is configured, packets is processed in software and a log message indicating this is generated:

  ```
  %C4K_HWACLMAN-4-ACLHWLABELERR: Path (in :50, 1006) label allocation failure:
  SignatureInconsistent - packets will be handled in software, QoS is disabled.
  ```

  One feature combination that can trigger this problem is the attempt to combine a QoS policy that matches on cos bits with IPv6 ACL configuration that matches on IPv6 source addresses that partially mask in the lower 48 bits of the address. (IPv6 subnets in the /81 to /127 range will also trigger this behavior if IPv6 multicast routing is enabled.)

  Workaround: Do not configure feature combinations that conflict. Currently the above conflict between QoS policies matching on COS bits and IPv6 configuration with partial masking of the lower 48 bits of the source address is the only known conflicting feature combination. If matching on COS bits is required by the QoS policy, architect the IPv6 network using /80 subnets or larger. (CSCsk79791)

- The **ip icmp unreachable** command may affect ICMP unreachable generation for both IPv4 and IPv6 packets received on the Layer 3 interface. Furthermore, a Layer 3 deny ACL on a Layer 3 interface with an IPv6 address may not copy the denied traffic to the CPU, bypassing ICMP unreachable generation.

  The first problem occurs on a dual Layer 3 interface where both IPv4 and IPv6 address are configured. The second problem occurs when all Layer 3 interfaces in a switch are configured with IPv6 address only.

  Workarounds: Avoid using a dual Layer 3 interface with both IPv6 and IPv4 address configured.

  Avoid using a switch as a purely IPv6 Layer 3 interface-only router. Ensure that it has at least one Layer 3 interface per SVI with IPv4 address configured. (CSCsk77234)

- When you toggle an interface configuration from a Layer 3/router port to a Layer 2/switch port, and then to a Layer 3/router port, an IPv6 ACL attached on the original router interface may not get flushed properly in the TCAM hardware even though the router interface's IOS configuration is unconfigured.

  Workaround: Before switching a Layer 3 interface from a router port to a switch port, unconfigure the IPv6 ACL on the router interface. This ensures that the IPv6 ACL is cleaned up properly both in the IOS running configuration as well as in the TCAM hardware. (CSCsk60775)

- The LEDs on E-series supervisor and line cards remain green even when the module reports a critical or shutdown temperature alarm. The LEDs should turn orange or red.

  This occurs on all E-series line cards that report critical or shutdown temperature alarms. The actual temperatures and the alarm states are visible in the output of **show environment temperature** command.

  Workarounds: None for LED colors. However, when an alarm is raised or cleared, console log messages and SNMP traps are entered. Also, the current status of any temperature alarms are visible in the output of the **show environment temperature** command. (CSCsk57143)

- When a non-default duplex setting is applied to a FastEthernet interface and you upgrade from Cisco IOS Release 12.2(31)SGA to 12.2(40)SG, the duplex settings on FastEthernet settings are lost. The interface reverts to its default duplex setting, and the duplex setting no longer appears in the output of the **show running** command.

  Workaround: If non-default duplex settings are in the running config, note them prior to upgrading, and reapply them after the upgrade completes. (CSCsk83670)

- In policy map, if a queuing class with the **bandwidth remaining percent <>** command sits before a priority queuing class configuration, the **bandwidth remaining percent <>** command action is not applied on reload.

  Workaround: Re-apply the policy-map. (CSCsk75793

- If *exceed burst* is not explicitly configured for a dual rate policer, the **show policy-map** command displays “0” as the burst value.

  Workaround: Enter the **show policy-map interface** command to find the actual *exceed burst* value programmed. (CSCsj44237)

- On switches with redundant WS-X45-SUP6-E supervisor engines and WS-X4506-GB-T interfaces that have been configured to use RJ-45, the QoS configuration on the interface is ineffective after a SSO switchover. Furthermore, you may lose the QoS configuration if the media type is changed to SFP and then back to RJ-45.

  The QoS configuration is present in the running configuration but is not honored on the interface.

  Workaround: Reapply the QoS configuration to the interface. (CSCsm58839)

- If you configure IPv6 MTU on an interface using the ipv6 mtu *mtu-value* command without first enabling IPv6 on the interface, your switch might pause indefinitely on startup.

  Workarounds: Before configuring IPv6 MTU on an interface you must enable IPv6 on the interface. To enable IPv6, use the ipv6 enable command.

  If you encounter this issue, use the following commands to recover your switch:

---

1. from the rommon prompt, use the **confreg** command to ignore the startup configuration
2. **reset** command to reboot your switch

3. **copy startup-config running-config** command to copy your startup configuration to your running configuration
4. **ipv6 enable** command to enable IPv6 on the interfaces
5. **ipv6 mtu** *mtu-value* command to configure IPv6 MTU on your interface
6. **copy running-config startup-config** command to save your recovered configuration
7. **reload** command on the switch to return to Rommon
8. from rommon, use the **confreg** command to process the startup config
9. reset the switch to resume normal operation. (CSCso42867)

- A switch directly connected to the uplink ports on a Catalyst 4500 supervisor engine does not see link down when the engine reloads. So, if UDLD is enabled, a link partner will enter the err-disable state.

  Workaround: Shut down supervisor uplink ports prior to reload. (CSCsl34390)

Troubleshooting

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

Netbooting from the ROMMON

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

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

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

2. Use ROMMON TFTP boot.

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

   – the BOOTLDR variable should *not* be set

   – the TFTP server must be accessible from the Ethernet management port on the supervisor engine.

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

a. Ensure that the Ethernet management port on the supervisor engine is physically connected to the network.

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

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

For example, to set the supervisor engine Ethernet port with an IP address 172.16.1.5 and IP mask 255.255.255.0, enter the following command:

```
rommon 2> set interface fa1 172.16.1.5 255.255.255.0
```

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

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

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

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

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

Troubleshooting at the System Level

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.
- Ensure that you do not mix the serial and Ethernet cables plugged into the supervisor engine. The Fast Ethernet port (10/100 MGT) on the supervisor engine is inoperative in all Catalyst 4500 Cisco IOS releases. An Ethernet cable plugged into the Fast Ethernet port is active only in ROMMON mode.

Troubleshooting Modules

This section contains troubleshooting guidelines for modules:

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

Troubleshooting MIBs

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

Related Documentation

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

- Catalyst 4500 Series Switch Documentation Home

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

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

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

Hardware Documents

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

- *Catalyst 4500 Series Switches Installation Guide*

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

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/catalyst4500e/installation/guide/Eseries.html
- For information about individual switching modules and supervisors, refer to the *Catalyst 4500 Series Module Installation Guide* at:

  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html
- *Regulatory Compliance and Safety Information for the Catalyst 4500 Series Switches*

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/regulatory/compliance/78_13233.html
- Installation notes for specific supervisor engines or for accessory hardware are available at:

  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html
- Catalyst 4900 and 4900M hardware installation information is available at:

  http://www.cisco.com/en/US/products/ps6021/prod_installation_guides_list.html
- Cisco ME 4900 Series Ethernet Switches installation information is available at:

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

Software Documentation

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

- Catalyst 4500 release notes are available at:

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

- Catalyst 4900 release notes are available at:

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

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

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

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

- *Catalyst 4500 Series Software Configuration Guide*

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

- *Catalyst 4500 Series Software Command Reference*

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

- *Catalyst 4500 Series Software System Message Guide*

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

Cisco IOS Documentation

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

- Cisco IOS configuration guides, Release 12.x

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

- Cisco IOS command references, Release 12.x

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

  You can also use the Command Lookup Tool at:

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

- Cisco IOS system messages, version 12.x

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

  You can also use the Error Message Decoder tool at:

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

- For information about MIBs, refer to:

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

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

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

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

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

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

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

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

Original SSLeay License:

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

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

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

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

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

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

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

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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

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

Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Release 12.2(46)SG1